An Architectural Approach for Command, Coordination, and Communications Capabilities Assessment

Kristin Lee
Sheila Cane
Salwa Abdul-Rauf
Carlos E. Martinez

The MITRE Corporation
McLean, Virginia

March 31, 2007

Approved for Public Release; Distribution Unlimited
MITRE Tracking Number: 07-0320

Abstract

This paper represents a follow-on to a paper presented at the 2006 Command and Control Research and Technology Symposium,[1] wherein the analytical methodology proposed in the prior paper has been improved upon and implemented in a relational database to support a variety of analyses related to command, coordination, and communications capabilities. In particular, relationships among the various major architectural components of a large-scale organizational enterprise are modeled, including:

- Missions to be accomplished
- Organizations responsible for accomplishing the missions
- Activities performed by the organizations in support of their missions
- Information content needed to support execution of mission-related activities
- Operational services needed to support execution of mission-related activities
- Data representations used to implement information exchanges
- Software applications used to implement operational services
- Hardware platforms used to host software applications
- Facilities at which organizations reside
- Communications capabilities used to link organizational facilities
- Security capabilities needed to protect communications

The methodology explicitly uses the components of the Federal Enterprise Architecture (FEA) as a common means of reference and employs "pick lists" to ensure consistency of contents and facilitate automated analysis of database contents. The paper presents an overview of the underlying model and how the FEA Reference Models are used in support of command and coordination functional capability and gap analysis. The model has been implemented in a relational database management system (RDBMS), and through changes to data table contents, is adaptable to support analysis of other command, control, and communications capabilities such as those used by the Department of Defense.

[1] Carlos E. Martinez, Kenneth Mullins, and Karl S. Sullivan, "A Framework for Architecture-Based Planning and Assessment to Support Modeling and Simulation of Network-Centric Command and Control," Presentation Number C-147, 2006 Command and Control Research and Technology Symposium. June 2006.

Introduction

Command and coordination processes are inherent in government operations. Whether supporting a military mission entailing command and control of forces, or a civilian incident requiring coordination among various Federal agencies as well as state and local entities, communications capabilities are essential to the success of the operation. The practice of enterprise architecture (EA) is a strategic method that relates an organization's business processes to its technical assets. As the outgrowth of several enterprise architecture efforts, an architecture-based methodology was developed for the analysis of operational and infrastructure capability gaps.

The Federal Enterprise Architecture Framework (FEAF)[2] was used throughout the development and implementation of the methodology. The structure and content of the five reference models: the Performance Reference Model (PRM), the Business Reference Model (BRM), the Service Component Reference Model (SRM), the Data Reference Model (DRM), and the Technical Reference Model (TRM), influenced the development of a conceptual architecture model and served as the basis for standard terminology required for the analysis of existing capabilities.

The purpose of the methodology described in this paper is to analyze an existing (or *as-is*) communications and technology infrastructure, to assess how that infrastructure supports the business operations or activities of the enterprise, and to provide the means to make recommendations for what is needed for improvement, to support specification of the future (or *to-be*) requirements[3]. The success of such a wide-scale analysis is dependent upon the identification of the key factors that define the capabilities to be assessed as well as the quality of the data that describe those capabilities. This effort focuses on the information that supports business operations and the communications interoperability that enables interagency information exchanges. In this context, communications is used in the broadest sense, from telecommunications up to and including applications and information exchanges.

Analytical Objectives

The primary objective of this approach as depicted in Figure 1 is to determine whether an organization has adequate technical assets, or infrastructure, in order to support operational activities. Operational analysis should determine whether an organization has properly identified its functional partners and related information exchanges for a given activity. Infrastructure analysis should identify communications gaps based on operational needs. Overlaid on operational and infrastructure analysis, scenario-based analysis should reveal situation-dependent capability gaps. When *as-is* gaps have been identified, recommendations for changes to meet operational and infrastructure gaps can be made. When a scenario is incorporated into the analysis,

[2] More detailed information on the FEA Reference Models can be found at http://www.whitehouse.gov/omb/egov/a-1-fea.html.

[3] The focus of this paper is on the *as-is* portion.

recommendations can be made based upon a specific situation, or generalized across several scenarios. The analysis is iterative; i.e., it can be repeated to determine whether the proposed operational and technical changes for the *to-be* systems will address the gaps uncovered during the *as-is* analysis.

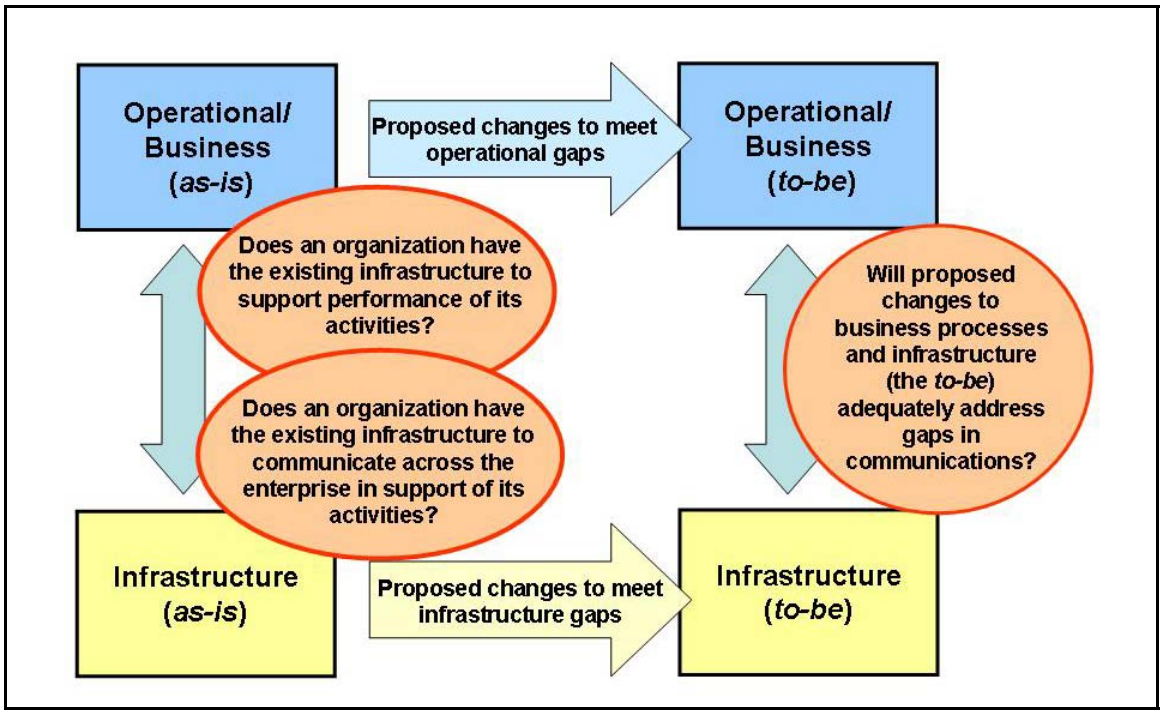

Figure 1: Analytical Objectives

An example of a wide-scale coordinated terrorist attack in the United States is introduced here to illustrate the utility of an architecture-based approach. The methodology is designed to be used to examine the extent to which local and Federal organizations that would respond to such an event have defined their operational partners and related information exchanges. An example question to be posed would be: have the local authorities identified which Federal agencies should be contacted in the event of a localized attack? Communications gaps can be identified as well. For example, do local first responders have a means to conduct voice communications with the proper Federal authorities? Do they have a means to transmit data in all required situations?

Conceptual Model

Essential architectural concepts including scenarios, organizations, operations, information exchanges, technical capabilities and locations were related in a high-level conceptual model. The model was divided into three primary domains: business operations, infrastructure, and situation, to help visualize and articulate the data needed to analyze how well the existing communications support the business operations and mission objectives during manmade or natural disasters. Separating the domains in this manner facilitates an independent analysis of each area as well as an assessment of the

impacts of changes to one area as they affect the enterprise. The three major analysis domains are shown in Figure 2.

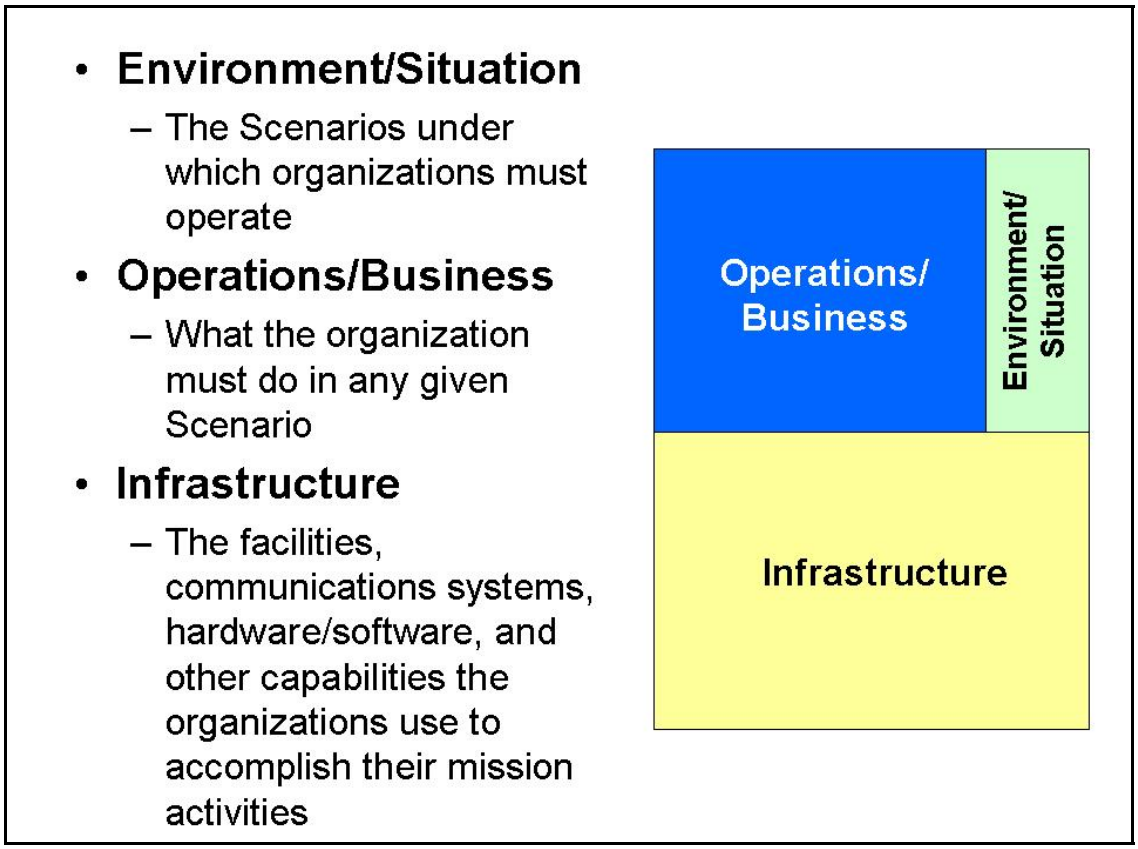

Figure 2: Major Conceptual Model Analysis Domains

Figure 3 demonstrates how the three domains were decomposed and conceptually modeled. This conceptual model is a high-level representation of the elements of importance and the relationships between them that are significant to the analysis needs. The domains are related in that infrastructure elements support the operational or business functions, and the environment or situation affects both operations and infrastructure. The conceptual model is meant to be a general representation of an enterprise with a command or coordination mission, and is viewed as the framework upon which the enterprise data is collected and analysis is performed. The conceptual model provides the basis for development of a database to store and analyze enterprise data.

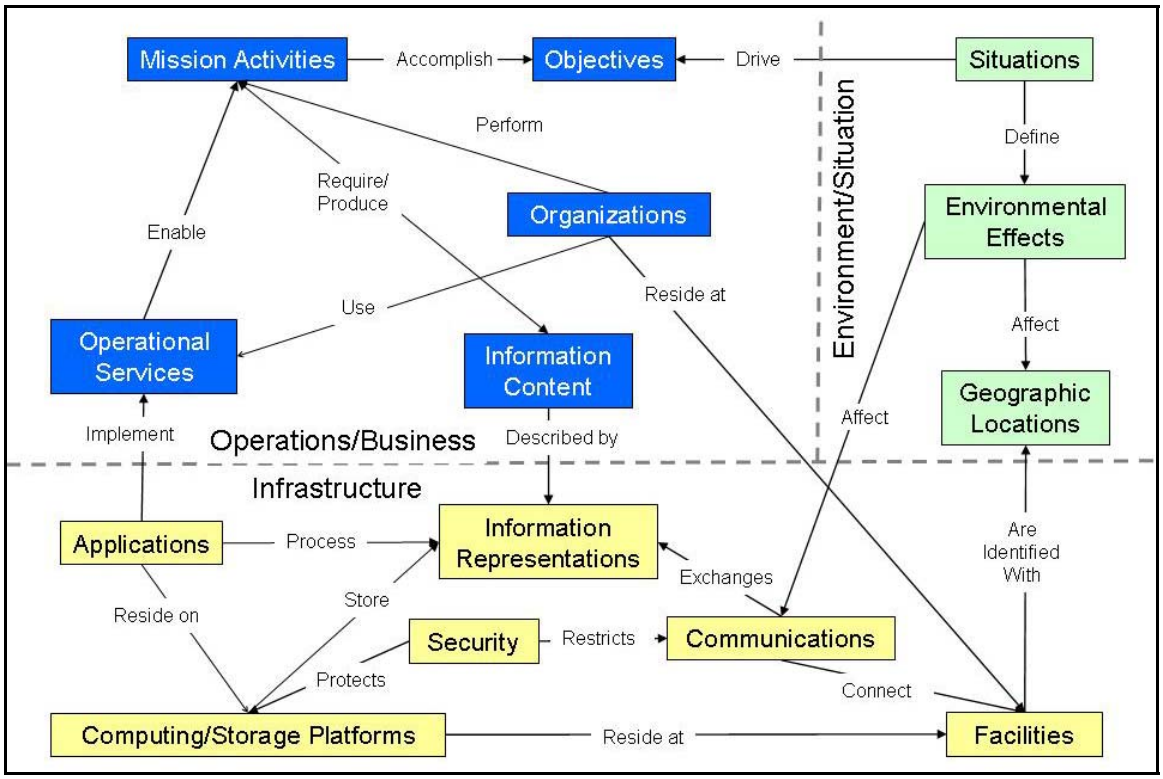

Figure 3: Conceptual Model

Operations/Business Domain

The business or operations perspective consists of the objectives to be accomplished by the mission activities. The blue boxes in Figure 3 define the operational area of the conceptual model. Organizations perform relevant activities by utilizing operational services in the business context of a mission activity. Information content consists of data that is required from (or produced by) an organization performing an activity.

Objectives represent the high-level goals of the enterprise, and mission activities are the enterprise business functions performed. Upon implementation of a database, mission activities can be further decomposed to include the sequence in which they are performed. The methodology presupposes that objectives and activities have been properly defined by the enterprise and its constituent organizations; there is no capability to check for inconsistencies with existing legal, policy, or strategic documentation.

Organizations are limited to those entities responsible for achieving business objectives. Organizations may be from any level of government from Federal to the state, local, or tribal level, or a non-governmental or international organization such as the American Red Cross or the North Atlantic Treaty Organization. Individuals such as the President and other senior leaders also fit the definition of an organization.

Operational services define mechanisms that enable an activity. As described in the Federal Enterprise Architecture (FEA) Service Component Reference Model (SRM), organizations utilize a wide range of services from support services such as systems management to analytical services like visualization. Operational services define the application requirements of the infrastructure domain.

Information content describes the information exchanges required from or produced by activities. An information exchange is a one-way transmission of data from one organization to another. Information content is defined by an enterprise-specific taxonomy. The exchange can be an input or output, is contained in a format and may be given a security classification. The information format and classification drive the communications capability requirements.

Following the example of a domestic terrorist attack, the first responder's objective is to save lives and protect property. First responder activities include securing the scene and conveying situational reports to the local fusion center. The fusion center in turn utilizes operational services such as knowledge capture of alerts and notifications to synthesize the situational information and notify appropriate Federal agencies. Example information exchanges may include reports, such as facts or statistics, or requests for guidance.

The operational and business domain conducts activities in support of the overall enterprise objectives. In doing so, this area drives the requirements of the supporting infrastructure by defining the situation-specific needs for command and coordination capabilities such as situational awareness and decision execution.

Infrastructure Domain

The infrastructure perspective depicts the tools utilized to facilitate the conduct of the business's operations. The elements in this domain provide the required communications capabilities from telecommunications assets, to computing platforms and applications, as well as the facilities at which they reside. The yellow boxes in Figure 3 represent the infrastructure elements.

Facilities represent the physical location of organizations and their communications assets. Facilities are not limited to fixed, ground locations, but include airborne and watercraft as well as mobile and transportable platforms. The facilities element contains location attributes key to a scenario-based capability assessment.

The communications element defines the means to exchange information between facilities, and covers the full spectrum of telecommunications from wireline circuits to terrestrial wireless to satellite communications. Information on existing communications provides the baseline for the capability gaps analysis; without a shared communications capability there will always be an operational gap between two organizations.

Information representations, applications, and computing and storage platforms are interrelated infrastructure elements. Information representations describe the format in which the information content is presented. Information representations are defined by broad format categories as well as specific standards. An example format is video, which includes the category for the standard MPEG-4. Information representations are the technical analogy to operational information content and provide one of two possible links between the business and infrastructure domains. Applications are required to process information representations. Applications implement operational services that enable activities in the operational domain. Applications, while not required for all communications, can provide the second of two links between the business and infrastructure domains. Applications reside on computing and storage platforms that are in turn located at facilities. Combinations of computing platform, application, and information representation add a level of complexity to the capability gaps analysis; each one may add another chance for incompatibility.

Security is necessary to protect the often sensitive information required of command and coordination operations. The approach recognizes the ubiquity of security; however, this element defines the physical security mechanisms, such as Type 1 encryption, that isolate communications and protect computing and storage platforms. It is worth noting that while security is modeled separately, it also appears as either an attribute or category in the majority of the conceptual model operational and infrastructure elements.

Continuing the example of the domestic terrorist attack, the first responder may use a radio with a specific waveform standard in order to share information with the fusion center. The fusion center is located at a facility that contains a mainframe on which an analytical application resides. The application is used to generate a report that is transmitted to a Federal agency via a secure means of communication.

The infrastructure domain provides a straightforward framework in which to document the technical assets of the enterprise. As a whole, the infrastructure domain supports the operational domain and is the primary focus of the capability assessment.

Environment / Situational Domain

The situational perspective consists of the scenarios that define environmental effects as well as missions that may drive or impact the enterprise objectives. The scenarios may be natural (e.g., major hurricane or pandemic influenza) or manmade (such as a terrorist attack), and the resultant effects may have varying levels of impact at differing geographic locations where the enterprise operates. The green boxes in Figure 3 represent the situational elements.

Use of the FEA Reference Models

The FEA reference models influenced the development of the conceptual model (Figure 3). The White House Office of Management and Budget developed the FEAF and related reference models to provide a set business-driven standardized terminology to be used across the Federal executive branch. The purpose of the FEAF is to aid cross-agency analysis of information technology investments to identify duplicative efforts.

The operational domain is compliant with the BRM and DRM. The BRM was used as indicated by the DRM to define the "Business Context" and "Subject Area" of the enterprise information exchanges. The business reference model instantiated by the conceptual model is described by the mission activities and objectives. For a Federal government-wide study activities should be related to the Lines of Business as defined in the FEA BRM. The portion of the conceptual model that serves as the BRM is shown in Figure 4.

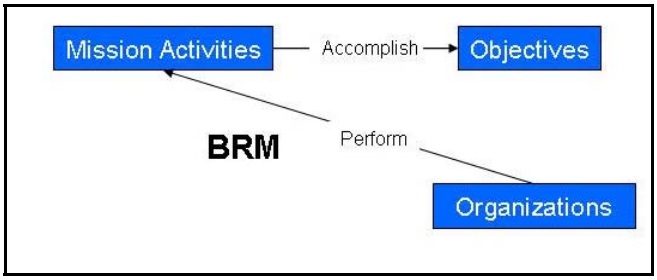

Figure 4: BRM application to the conceptual model

The DRM was applied to the information content and information representation entities of the conceptual model. As recommended in the FEA, broad types of information exchange were defined (e.g., report of facts or statistics, request for authority, financial transaction). The information exchange content types are linked to information representation by relating which information representation standards meet the information content needs. The relationship of the DRM to the conceptual model is shown in Figure 5.

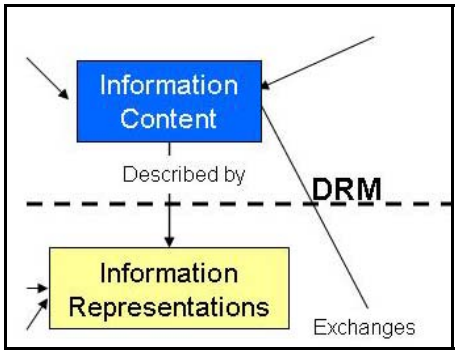

Figure 5: DRM application to the conceptual model

The PRM can be used to identify enterprise-level metrics used to assess operational performance of the mission activities; for example, timeliness of an activity initiation during an emergency. Performance metrics can also be used to measure the success of a sequence of activities as they relate to a defined process flow. The PRM spans the entire conceptual model.

The SRM applies to both the operational and technical areas and was used to define the operational services pick list. The SRM was also used as a reference for developing the applications-related part of the data model and the applications pick lists, and shows how applications meet operational needs. The relationship of the SRM to the conceptual model is shown in Figure 6.

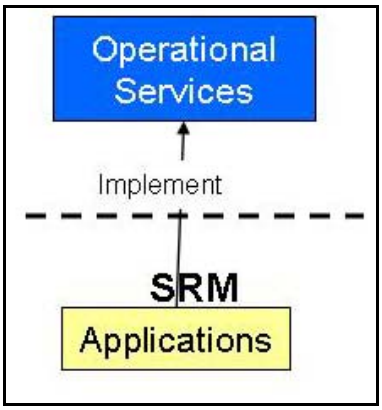

Figure 6: SRM application to the conceptual model

The TRM was used to inform the technical area of the conceptual model. The TRM influenced the structure and content of the infrastructure pick lists. It was also used in defining types of communications capabilities and their attributes. Via the links to applications and information representation, the TRM shows how the technical infrastructure meets the operational needs. The relationship of the TRM to the conceptual model is shown in Figure 7.

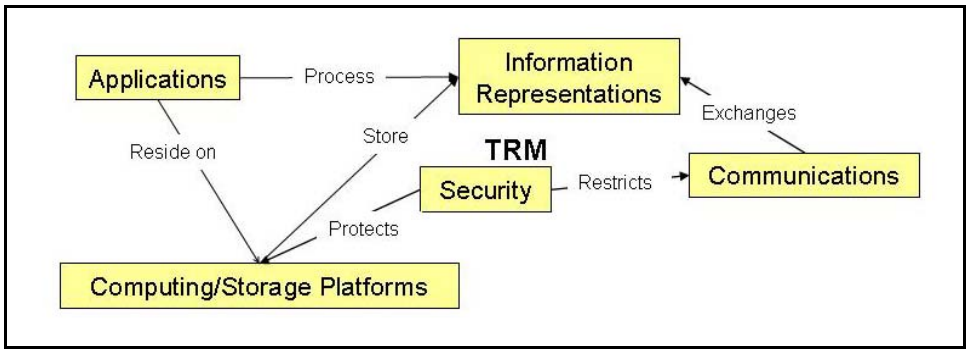

Figure 7: TRM application to the conceptual model

Analytical Framework

The key factors from the conceptual model that are involved in interagency operations are laid out in sequential order in the analytical framework pictured in Figure 8. On the left side of the figure, for a given mission an organization must perform specific activities. These activities require information that is defined by the enterprise taxonomy. On the right side of the figure, another organization, through its own activities, produces the information content to be consumed by the first organization. Information content is represented using standards and is processed by applications. The information may be protected by security measures and then transmitted via some means of communication. The information flows up through infrastructure elements to the information consumer. The sequence presented in Figure 8 represents the set of technical capabilities that support an information exchange. The analyses defined herein are not intended to be performed in real-time, but instead to understand the exchange of information between organizations at several levels and to serve as a strategic planning tool.

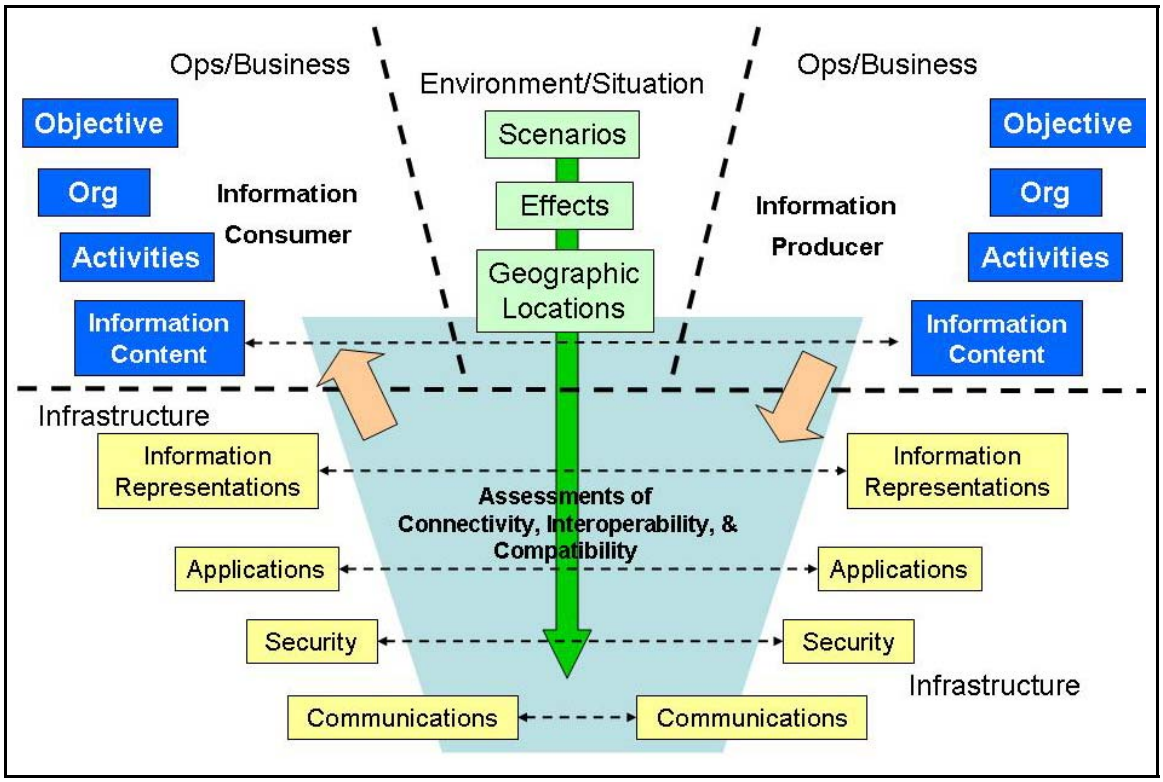

Figure 8: Analytical Framework

Assessments of connectivity, interoperability, and compatibility of communications capabilities occur in the infrastructure portion of the analytical framework. Starting from the bottom with communications, the analytical framework provides a systematic approach to determining capability gaps within the enterprise; as the analysis moves up the framework another layer of complexity and possible

incompatibility is added. The elements build on each other, and the possible domain values of each are defined by those below it. For instance, the set of security devices that can be used to protect an information exchange is defined by the means of communication. By scoping the analytical process in this manner, once a gap is identified, the analyst may stop and develop a mitigation strategy. The viability of the proposed solution can be tested using the same process, and once the gap is closed the analysis can continue at the next level up in the framework. The intent is for the analysis to be thorough and iterative.

The analytical framework in Figure 8 also includes "what-if" situational analysis. Scenarios have effects on certain geographic locations. Depending upon the scenario, there may be negative impacts on the facilities identified with these locations. While facilities and computing platforms are not explicitly modeled in the analytical framework, their resiliency and robustness affects the infrastructure components that are related to them. Assessing the impact of environmental effects on locations can identify potential infrastructure vulnerabilities. Given a hypothetical infrastructure breakdown, the analytical process will help to identify the impact of the scenario on enterprise objectives. The results of such a scenario analysis are critical for the development of a *to-be* architecture that supports the operation of enterprise missions under all conditions (such as command and coordination activities).

Additional operational analysis can be performed on the enterprise objectives. Pair-wise assessment of organizational activities and information requirements can determine whether organizations have properly identified their operational partners. An enterprise-wide information exchange analysis can discovers gaps such as information requirements that are not met, or information that is generated, but not used. This operational analysis provides a means to streamline enterprise operations by identifying gaps and redundancies in mission-critical information flows.

The response to a wide-scale, coordinated domestic terrorist attack can be used to illustrate the types of assessments defined by the analytical framework. The regional fusion center requires intelligence information from the Federal Government on individuals who have claimed responsibility for the event. Hypothetical examples of capability gaps can be identified at each level in the analytical model for this scenario. For example, the required information may reside on a data network that a Federal agency and the fusion center do not have in common. The information may have a higher classification than the level at which the fusion center is accredited. The Federal agency may synthesize the data using a newer version of an application which is not backwards compatible with the older version that is at the fusion center. If the Federal agency and fusion center required a video teleconference to discuss the situation the locations would need to use compatible video encoding standards. The Federal agency may successfully transmit the data to the fusion center, but the information may not have the attributes that the local authorities require; this represents an information content gap. The organizations may be in the process of exchanging information when a second attack occurs near the fusion center, cutting the fiber in the access circuits to the facility. The fusion center would need to have backup communications such as a satellite capability in

order to continue coordinating with the Federal agency. Using the analytical methodology as a part of a strategic planning process would identify these potential gaps, and the organizations could develop technical solutions in preparation for such a scenario.

Design Concepts and Implementation

In developing a solution that would support the analysis to be conducted, various EA tools were considered. Two key requirements were clear from the outset: the tool must have a strong query capability and must provide flexibility in building the underlying data model to meet the projects' information needs. Several EA tools were evaluated and found to be unsuitable for the analytical needs because each had a closed architecture, their own internal query language, and custom methods to modify the underlying data model. It was decided that the best approach would be to use a relational database management system (RDBMS) where custom queries can be developed using a standards-based query language such as Structure Query Language (SQL), and data can easily be passed to any visualization tool to support analysis through standards such as (comma separated values) CSV files. The development and use of a standards-based RDBMS repository rather than an off the shelf EA tool can:

- Enable capture of all relevant enterprise data
- Facilitate data collection
- Support compatibility and gap analysis objectives, and
- Provide traceability to the FEA reference models

To facilitate development of an architecture repository, the components defined in the conceptual model (Figure 3) were further defined by a detailed entity relationship diagram using standard data modeling techniques. Each entity was broken down into one or more physical tables. These tables contain the attributes including the key data that uniquely defines each entity. The tables are interrelated and linked in the model. The conceptual model can be applied to a myriad of architectural analyses. Similarly, the detailed data model may have many attributes in common, but in some cases will be project-specific as individual programs and missions have different data needs and attribute definitions. In particular, while different organizations re-using the conceptual and detailed data models may have significantly different operational activities, their technical infrastructures may have many components (attributes and data) in common.

A portion of a physical data model developed using this architecture-based methodology is shown in Figure 9. The organization element of the conceptual model was decomposed to organizations, branches, and organization types. The "_PL" at the end of each entity name indicates that the entity is implemented as a pick list. Pick lists are used to maintain data consistency across organizations, i.e., to prevent the same organization from being represented using different names. To ensure consistency across the data compiled in a large-scale organizational enterprise, standards in the form of pick lists should be used. These lists consist of the standard taxonomy to be used across the enterprise. Any enterprise data must be documented in terms of this taxonomy. For

example, the table entitled 'Org_PL' in Figure 9 contains all of the enterprise organizational data; that is, only the records stored in the physical instantiation of this table are valid enterprise organizations. The utilization of common terminology facilitates analysis. A SQL-based query would not know that the terms 'Department of Defense' and 'DoD' refer to the same organization, and could overlook key linkages in the data. Every instance of an organization must use the same name, which is stored in the 'Org_PL' table.

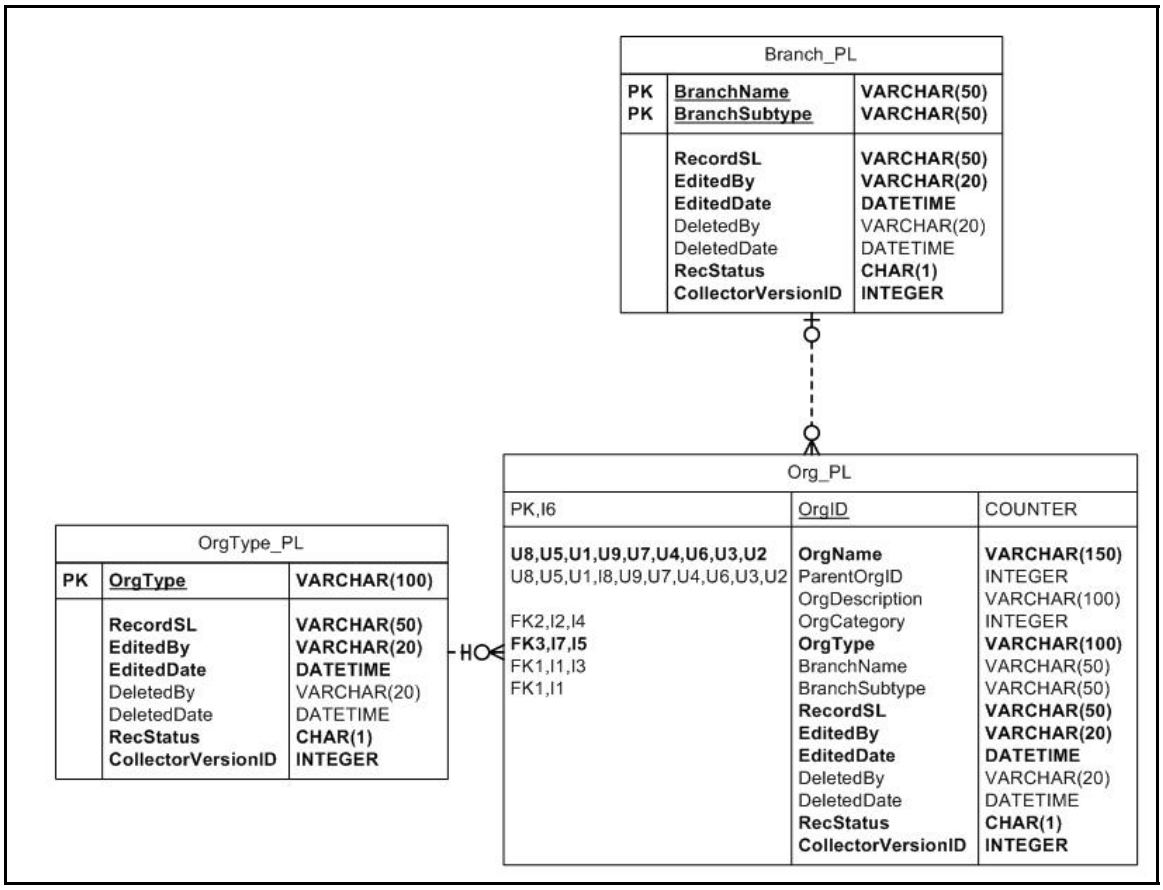

Figure 9: Representative Physical Data Model

The data model in Figure 5 also shows data and administrative attribute definitions and entity relationships. The implementation of the organization provides for a hierarchical organizational structure by relating an organization to its parent. For example, the Department of Justice as the parent organization of the Federal Bureau of Investigation can be represented by this structure.

Future Work

The data model is being extended to include activity sequencing, so that upon implementation of a database, mission activities can be further decomposed to include the sequence in which they are performed. The degree to which the activities and process

flow are decomposed will be dependent upon the requirements of the analysis to be performed.

Operations centers represent a special case of organization, as they consist of multiple, independent, co-located organizations that may interact with other such centers or individual organizational entities. The data model will be enhanced in the future to update the definition of an operations center as an organization with specific skill sets.

Summary and Conclusion

There are several benefits to be achieved by utilizing an architectural approach to assess communications capabilities. These include a the development of a general framework upon which analysis of interoperability, compatibility, and communications gaps can be performed, and the ability to assess the relationship of supporting infrastructure to operational activities. The results of the analysis can provide valuable inputs to an enterprise's strategic planning process. The use of pick lists inspired by the FEA enables data standardization by providing data consistency which will facilitate analysis. The use of a standards-based RDBMS provides an open architecture that permits program-specific data definition and provides the ability to perform custom database queries.

Appendix A

Lessons Learned from Use of Reference Models

While the complete set of FEA reference models were not used explicitly, they were useful in standardizing terminology for data collection and analysis. The reference models saved significant effort by providing a pre-defined set of business and technical terminology with which the project could start.

The BRM was useful for categorizing information needs and identifying relevant activities. Detailed data modeling across the enterprise was not attempted because it was viewed as too complex for wide-scale organizational enterprises. The DRM recommendation to use the top two levels of the BRM and then add detail was helpful in generalizing information content across organizational contexts; for example, information content was modeled as classes of information such as guidance or direction, rather than modeled as specific data elements. This approach may be more appropriate, and is certainly more feasible for multiple enterprise analysis.

Using the SRM proved somewhat difficult because it includes a mix of operational and application services. It was not readily apparent which services belonged in the operational services category and which services belonged in the applications category, thereby limiting its usefulness for pick list development.

The TRM was an excellent stating point in the development of the infrastructure pick lists because it provides ideas for technologies and standards that should be considered. However, the technology lists provide a limited set of examples and do not provide enough detail within the categories.

The PRM provides useful categories of metrics to measure operational improvements, for example. However, the lack of concrete examples makes it difficult to implement.