2006 CCRTS
STATE OF THE ART AND THE STATE OF THE PRACTICE

C2 Policy Track

National Command Capability
Design for a
Collaborative Environment

Peter H. Lyon
David Dick
CACI-National Security Research, Inc.
2231 Crystal Drive, Suite 500
Arlington VA 22202
(703) 647-2200
plyon@caci.com
ddick@caci.com

Abstract

National crises demand that leadership deliver an effective response that requires: timely alerts and warning, accurate information on emerging situations, the ability to consult with distributed partners, advisors, and specialists, the ability to collaborate with authorities in various jurisdictions, the ability to secure and contain the crises, the ability to organize and deliver resources to those in greatest need, and the ability to show leadership and support to the people. The NCC solution is to create the virtual "collaboration environment" of software and hardware capable of delivering a host of services and applications to anyone with a web browser. The NCC also provides a "trusted information environment" that allows leadership to perform all critical functions in the event of threats spanning local and regional incidents to those of national significance.

This paper describes an approach to bring urgent progress in these areas within a single unified framework for command capability. This NCC architecture framework can lead progress in SOA architecture as a distributed network standard. By taking advantage of current models of technology and technology partnerships in the private sector, this NCC design can inspire rapid deployment, early adoption and innovative growth in support of cross agency information sharing.

Background

The President of the United States has directed improvements be made to the nation's ability to respond to and manage crisis situations involving multiple agencies at the federal, state, local and tribal levels. Such improvements would deliver a robust national command and control capability that is fully interoperable with regional and local command and control systems. We have the means and now, in light of recent events, we have the will to enable effective and appropriate response to a full range of emergencies and disasters. Naturally, an interoperable capability of this strategic importance must be both nimble and survivable.[1] Fortunately, unprecedented innovations in enterprise integration, open systems architecture, data modeling and extended distribution networks make such a capability possible. The opportunities exist now to apply proven technology and engage in technology partnerships to explore emerging innovations that will achieve a successful capability framework.

The current National Command Capability (NCC) has grown from several directives and policy initiatives in recent years. The current NCC initiative was originally inspired by a National Security Presidential Directive-28 (NSPD-28), entitled "United States Nuclear Weapons Command, Control, Safety and Security." Further support for this initiative was provided by Executive Order 12472, "Assignment of National Security and Emergency Preparedness Telecommunications Functions," which emphasizes the need to ensure that "a national telecommunications infrastructure is developed which: (1) is responsive to the national security and emergency preparedness needs of the President and the Federal departments, agencies and other entities, including telecommunications in support of national security leadership and continuity of government; and (2) is capable of satisfying priority telecommunications requirements under all circumstances through use of commercial, government and privately owned telecommunications resources."

Executive Order 12656, "Assignment of Emergency Preparedness Responsibilities," states "[t]he policy of the United States is to have sufficient capabilities at all levels of government to meet essential defense and civilian needs during any national security emergency. A national security emergency is any occurrence, including natural disaster, military attack, technological emergency, or other emergency, that seriously degrades or seriously threatens the national security of the United States."

The current NCC effort is led by the Department of Homeland Security (DHS), in coordination with the Department of Defense (DoD) through an Interagency Task Force for NCC (ITF-NCC). The ITF-NCC will initially be represented by and report to the Nuclear Command and Control System Committee of Principals (NCCS CoP). The ITF-NCC is chaired by DHS and vice-chaired by DoD, Assistant Secretary of Defense for Networks and Information Integration (ASD NII). The ITF-NCC will operate in a collaborative fashion with all Federal Executive Branch departments and agencies, as defined in the new Federal Preparedness Circular (FPC) 60. The results and recommendations of the ITF-NCC will be coordinated with the Executive Office of the President (NSC, HSC, OSTP and OMB) and presented for approval to the NCCS CoP.

[1] See Appendix sections and Authorities and References section for supporting details.

An earlier effort to model an agile C2 capability within a Net-Centric environment was conducted in 2003 with follow-on update completed in 2004 [2]. This study of a "Unified Command Structure (UCS) Command and Control Capability" was completed in two parts, first a detailed review of a the "2004 Baseline As-Is" and second, an objective "To-Be" operational and systems view for capabilities expected in 2010.

While not as detailed as the "UCS" effort, this paper follows a similar scope for a national C2 capability and builds on some systems interface descriptions discussed, notably the institution of "systems nodes" that represent communities of interest(COI) and representative interfaces between the COI nodes and the "Net-Centric Information Environment" (NCIE).

Concept

This paper proposes an NCC architecture framework intended to support the missions described above. This approach to collaborative technology will deliver the essential functions of government extended across many communities of interests (COI) to enable effective interoperable command and control capability. The primary focus in this NCC architecture is to implement features that support C2 collaboration across governing organizations while fusing characteristics of C2 agility in the framework. In this way, NCC concept can provide information sharing, situational awareness, collaborative decision-making, and coordinated land-air-sea-space operations across all government organizations. In becomes a way for leadership to take responsible, decisive action during critical situations.

Introduction – Motivation for a Unified Design

To create a unified framework serving all sectors, a blend of integration models from private and public sectors is necessary. Events within the past 4 years however, have put even greater urgency on realizing a shared network that reaches both public and private sectors. The immediate challenge is to identify the technology models that are sufficiently agile, adaptive and highly integrated.

For over ten years initiatives have been underway to engineer an almost transparent enterprise architecture built on the principals of collaboration and sharing. Yet the collaboration process between public and private sectors has been hampered by an ambivalent relationship. Private industry is motivated by free market economics and a fierce motive for profitable market share. Technology innovations are the fruit of shareholder investments in R&D while successful deployment and implementation becomes the realization of greater market share. Government and defense organizations, on the other hand, have a long history of partnering with industry to engineer break through technology. When this collaboration succeeds and is well funded, public agencies gain efficiency and private industry gains market share. When experimentation fails, the level of effort invested simply becomes the cost of doing business.

[2] DISA, "*Unified Command Structure (UCS) – Objective Architecture Views",* Draft 2004.

Today, businesses have achieved remarkable success in making enterprise application services work across previously isolated systems, something only possible through coordination among stakeholders and technology engineers. This has lead to a powerful change in incentives that now encourage organizations to work together. Collaboration within the enterprise is now understood as a pre-condition of survival in a global market.

The objective of this paper is to identify the opportunities before us today that can succeed through a joint partnership to lead the way towards building a National Command Capability that can be inspired by organic growth and an expanding national community.

The NCC Model – Survival in Partnerships

Bringing applications and services across a shared and increasingly converged network is no longer theory; examples of success are evident in pilot programs and initiatives across many government agencies and DoD organizations. Likewise, many familiar names in the commercial sector are promoting integration solutions. Understandably, new products intensify the competition and bring more pressure on stakeholders and engineers to push innovation further still. Innovation, as it turns out, requires collaboration, so ultimately successful growth and development simply means more partners. This is especially true for innovations based on open source architecture that promise interoperable solutions.

A recent example is the partnership for standards initiated by Iona Technologies in November 2005. Together with industry competitors, Bea Systems, IBM Corporation, Oracle, SAP and Siebel Systems (among others) Iona seeks to define a common "SOA Programming Model".[3] This presents a modern paradox where natural competitors are discovering the path to survival lies in cooperation.

The NCC architecture framework must gain from these partnering initiatives as it seeks proven technology and models of interoperability. In fact, the early design of NCC architecture should be narrowed in scope by just those technologies that are proven and viable. To ensure the NCC model is successful however, this "base function set" must also incorporate features of an "Agile C2" system as described by Dr. David Alberts in several CCRP publications.[4] The dimensions of agility (as identified in "Power to the Edge") are;

- Robust
- Innovative
- Flexible
- Resilient
- Adaptive
- Responsive

In this way, the NCC architecture must extend beyond the traditional notion of an enterprise system to become a framework of extended networks joined by collaboration agreements. It is within this context that the discussions of this paper will be framed. The next several sections identify several phases of enterprise architecture (illustrated in Figure 1) followed by concluding sections that review the dimensions of success for NCC.

[3] Press Release, Iona Technologies November 15, 2005.
[4] Alberts, D.S, Information Age Transformation, Getting to 21st Century Military, CCRP Publications, 2002 (pp 82)

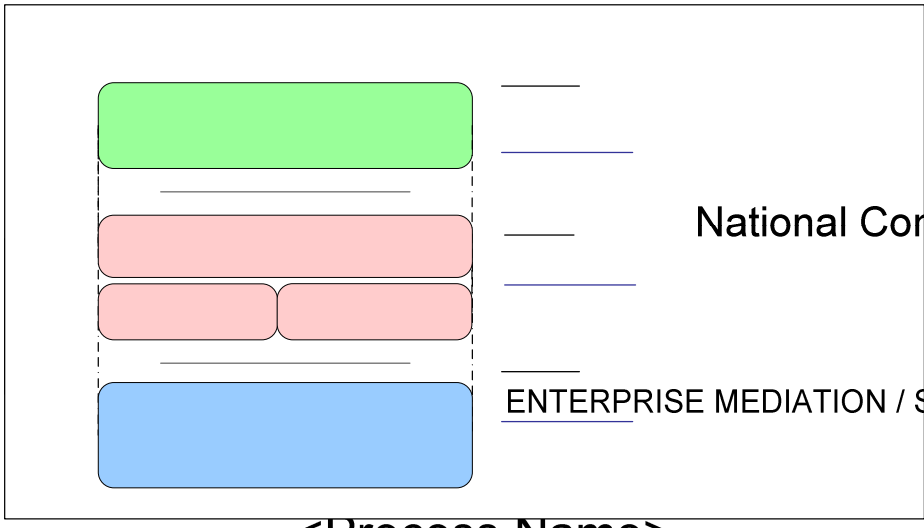

Figure 1. NCC enterprise capability, organized by "integration phases".

The first discussion will identify approaches to "Enterprise Mediation". This will identify solutions for managing the myriad of transactions and services within the NCC architecture framework.

The next topic will cover "Web Applications and Services" and will drill down to solutions for data sharing, common registries and message patterns that are the foundation of enterprise integration and service oriented architecture. The last section of this part will review the convergence of "Shared Knowledge and Distribution Network" as it relates to a distributed NCC architecture framework.

The three concluding sections of this paper focus on the organizational nature of the NCC architecture framework. These will explore the "NCC Success Model" as it relates to a "Trusted Environment, "Organic Growth" and finally, "Certification".

Enterprise Mediation & Governance: NCC as Robust and Resilient

A brief survey of existing integration models will help define a practical scope for the NCC architecture framework as a "base function set". These "mediation and governance" models provide the basis for sharing data and services within an enterprise architecture. Several commercial examples of mediation models are noted in the figure below.

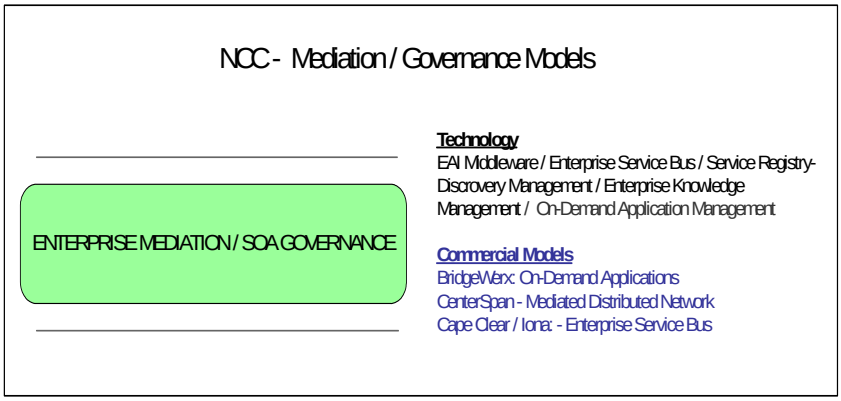

Figure 2. Mediation and governance models are occasionally thought of as "content distribution" solutions. Some examples include BridgeWerx and CapeClear mediation products.

NCC Base Functions: The foundation architecture and design of a NCC will use open system architecture and inspire growth through user participation. There are many federal standards and policy documents that identify models of technology, interoperability and data modeling. However, the minimum NCC functions will focus directly on essential Net-Centric operational concepts that "…depend upon the ability to exchange information ubiquitously among network participants…"[5] Specific guidance for implementing Net-Centric compliant capabilities is described in "Net-Centric Checklist" published by OASD (NII)/DoD CIO.[6] Moreover, the technology models of SOA will ensure alignment with federal reference models similar to the DoD Net-Centric Operations Warfare Reference Model and the Federal Enterprise - Data Reference Model.

More importantly, SOA represents an architecture that is scalable, robust and resilient. Since an SOA design supports loosely coupled "services" that interoperates to perform defined functions, it serves the NCC requirements to be flexible and adaptive. It provides timely, relevant, accurate information to an unlimited community of consumers and in this way relies on innovation that will prove to be responsive.

As the desire to support an ever-expanding community of users has flourished, so has the list of available solutions, even though the new solution names seem to be familiar integration strategies. Indeed, these solutions might be more accurately thought of as "sustaining innovations", the type of improvements for which success metrics have already been validated.[7] These approaches to integration simply reflect the new understanding of the "enterprise" although the technology may not be the transforming variety.

Early notions of an enterprise developed around the recognition of many independent software applications that should be serving a common business strategy. This became an exercise in Enterprise Application Integration (EAI). Responding to an increasing demand of business to allow "stovepipe" applications to exchange data, middleware components arrived to enable connectivity. "The demand of the enterprise is to share data and processes without having to make sweeping changes to the applications or data structures". [8]

Once EIA tools became increasingly object oriented, an approach to manage these as a whole emerged as the "Enterprise Service Bus" (ESB). A model similar to this approach is known as the Enterprise Services Integration Framework (ESIF). It is not surprising therefore, to see these approaches as part of the enterprise concept embodied in SOA.

Enterprise Service Bus (ESB) Essentially the ESB focuses on the ability to coordinate service requests with service providers while identifying the appropriate data source and applying data transformation as specified by the business logic. This approach to enterprise mediation delivers a critical role in managing the many processes and transactions in a way to preserve business logic and performance. This scalable technology can manage services across an unlimited enterprise of applications and services and easily extend to other

[5] Net-Centric Implementation Document: *"NCIC000"* – v 2.0 (Nov 28 '05) – Executive Summary
[6] "*Net-Centric Checklist"* – published by Office of the Assistant Secretary of Defense - NII-CIO, v 2.1.3, May 12, 2004
[7] Alberts, D.,Hayes, R. Campaigns of Experimentation, Pathways to Innovation and Transformation, a CCRP pub, 2005, - discussion of the "Nature of Innovation" (pp 41-62).
[8] Linthicum, D. Enterprise Application Integration, Addison Wesley, Reading, MA – 2000, (pg 3)

interoperable challenges like messaging, metadata and channel adapter mediation. Equally important, ESB models have proven effective in several programs within DoD already.

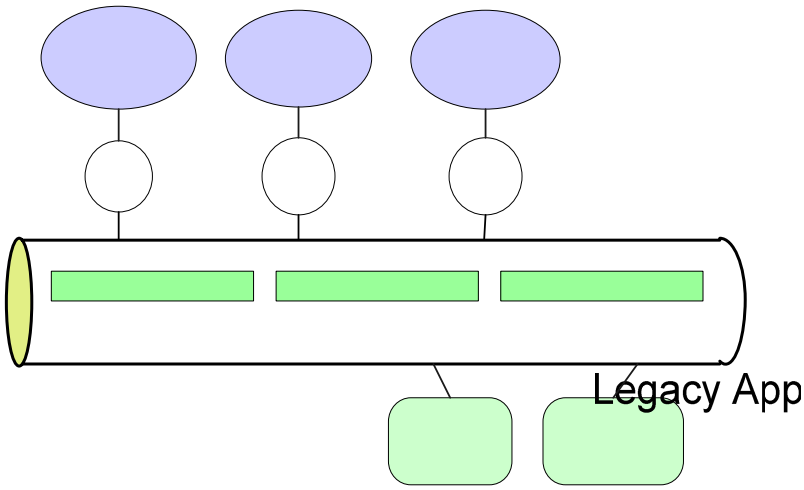

Figure 3. A compelling benefit of the Enterprise Service Bus is ability to scale this solution to accommodate expanding enterprise communities.

A chief benefit of services mediation models like ESB, is the scalable nature of applying this model across unlimited number of applications and services. The "bus" approach easily extends to other interoperable challenges like messaging, metadata and channel adapter mediation. Finally, this design is robust and resilient since it insulates the user interface layer, application layer and a data layer from one another – there is no single point of failure.

The ESB design has already drawn some interest in the Air Force. In 2004, the Air Force included an ESB designed as part of its Global Combat Support System (GCSS-AF) initiative. The design combined a number of proven solutions as part of a framework using JMS publish/subscribe, SOAP request/reply patterns along with IBM WebSphere Application Server and WebSphere MQ to deliver a robust solution designed to integrate multiple communities of users.[9] The significant difference here was the introduction of web services as a component of managing the processes of multiple distributed objects without interfering with existing enterprise exchange patterns.

There are a growing number of other commercial enterprise suites that tailor unique business rules and logic to an ESB framework. FileNet P8 Platform is an example of applying the ESB framework to accommodate a range of content and process management needs across an enterprise. The FileNet solution highlights a single enterprise catalog of content repositories from which service requests and providers are mediated. A key enabler of this model is the use of business logic to negotiate the enterprise services (available through a technology partner ILOG and their "J-Rules 5.0" product. Other commercial solutions marketed as ESB type mediation services include;

- Cape Clear: Service-centric ESB Platform

[9] Briefing Slides "*Integration and Enterprise Service Bus (ESB)"* for the Global Combat Support System (GCSS-AF) Summit – prepared by Lockheed Martin, December 2004 and February 2005.

- Bridge Werx: On-Demand Application Services
- Sonic Software: Orchestration Server and SOA Suite
- Iona Technologies: Open Source – SOA & ESB

Web Applications & Services: NCC as Flexible and Adaptive

The section to follow will look at existing and often proven mechanisms that promote shared services and exchange of data. Not only do these models manage the growing number of distributed objects, data, messages, and transactions and parameters governing business logic, they also support a system that is flexible and adaptable. For these reasons, these technologies are strong candidates for a NCC architecture design.

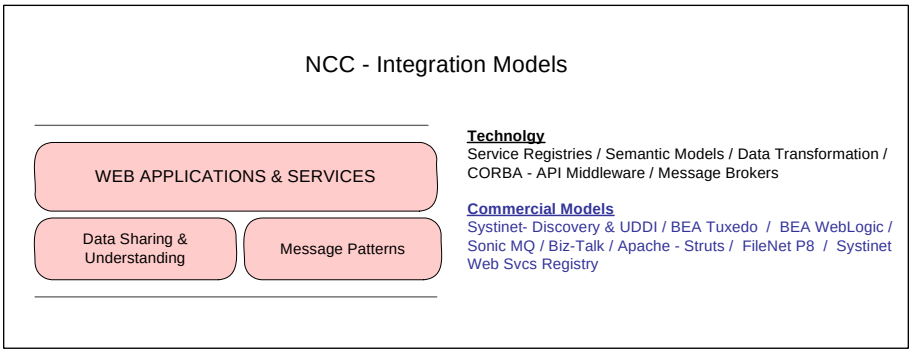

Figure 4. The "Integration Models" provide an array of message exchange patterns and transfer protocols.

Standards in exchange protocols exist, semantic translation adapters are proven and common service exchange models continue to appear in the commercial sector offering examples of integration models frequently used within an SOA solution .

In fact, it is this very rich environment of new and old innovations that present the fundamental challenge still before the NCC architecture. As attempts to establish a standard or "universal" approach to registration, discovery and exchange have largely failed, alternative concepts of developing an "execution context" have gained ground.[10] The exchange of services between providers and users is formalized by a description of the necessary "service interface" and agreement to use common exchange attributes that is, a "service contract".

The Unified Command Structure (UCS) study (mentioned in "Background" section) provides some detail on a number of exchange providers and users that may represent a similar "execution context". In fact specific inter-dependent activities among these COIs are further described in the "Operational Node Description" (OV2) as are requirements for information exchange (in OV3).

From an implementation perspective several of these types of exchange requirements may specify the COI's common exchange protocols and interface requirements, for example, Application Programming Interface (API), Remote Procedure Call (RPC), Universal Description Discovery Integration (UDDI), and Protocol Standards: TCP/IP, SOAP and

[10] OASIS - "Reference Model for Service Oriented Architecture" – Committee Draft v 1.0, February 7, 2006, (pg 21)

data exchange format XML. To the extent that both interface and contract requirements can be described in a way to permit "automated interpretation", it may be possible to avoid establishing a single standard for all to comply with.

Service Contract Language The interoperability "touch point" for the NCC architecture (as well as SOA in general) is how services connect. The enabling model, the "contract agreement", leverages a common description language, the Web Services Description Language (WDSL) and a corresponding interface connection.

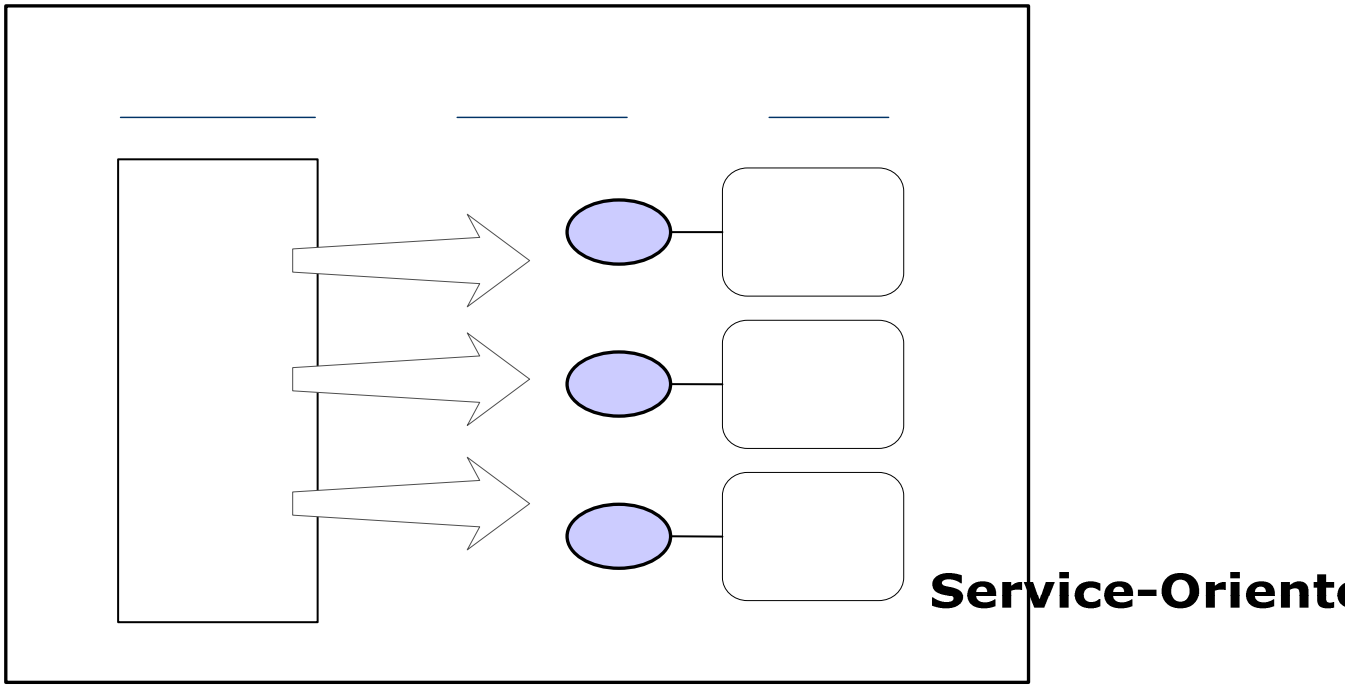

Figure 5. Establishing an understanding of the available service and the necessary service interface to connect, make up the basis for a "Service Contract" – the details of which are contained in the WSDL.

As a fundamental technique for enabling SOA, the WDSL serves to announce the existence of a service, provide a description of what it does, identifies its endpoint (physical address) and describes compatible interface connections. The illustration above shows the basics of successful interoperability. The service connection between provider and user is established once the contract is "agreed to".

If the service contract defines the agreement, then it is the transport mechanisms that enable the exchange. Both the service contract specification and a common set of protocol standards enable the core transactions for events and exchange of interoperable data.

Harnessing Middleware: The exchange of information between services and data sources depends largely on components that have been proven "integration elements" for years. This technology is still fundamental to many enterprise integration solutions and more importantly, supports functions that are flexible and adaptive.

A generation of integration "broker" architectures evolved that negotiated point-to-point connections, advertised limited network routing (Routing Information Protocol – RIP), and a new appreciation for Application Programming Interface (API) standards. The enabling middleware for these solutions included Object Request Brokers (ORB), Common Object Request Broker Architecture (CORBA) and standards for Interface Definition Language (IDL) software running on top of the operation systems.[11]

By the late 1990's, the Object Management Group (OMG), formed a partnership of industry organizations to define a "Model Driven Architecture" (MDA). This identified the best-known specifications at the time for data exchange including CORBA, XML and SOAP. Benefits and effectiveness of these standards and an evolving application language (Ada 95) were published [12]and eventually incorporated with the Defense Intelligence Agency's (DIA) Modernized Integrated Database (MIDB) program in 1998. A series of commercial solutions offered by Oracle – relational database structure, and IONA product, "Orbix-ORB" (and now, SOA – ESB products) collaborated with DoD to enable this initiative. Eventually this initiative included the Central Imagery Office's (CIO) Common Imagery Interoperability Facility (CIIF) as the primary imagery service used for the MIDB program. These models demonstrated effective use of distributed object management tools to produce a capability for seamless data access using CORBA, API and Ada 95. [13]

Many integration solutions still incorporate "legacy" enabler technology proven years ago. The ability to "wrap" older software applications allow them to appear as distributed objects. If these are Windows based, then using a Component Object Model (COM) is effective. However, if the enterprise has a decidedly heterogeneous (UNIX, NT, mainframe, etc.) platform, then CORBA is a productive distributed object standard to use.

A recent program for automated enterprise capability, Global Combat Support System – Air Force (GCSS-AF), incorporated several essential open commercial standards in their Integration Framework; CORBA, Java 2 Enterprise Edition (J2EE) and J2EE – Enterprise Java Bean (EJB).[14] Similarly, the need to support common data transfer methods is fundamental to continue providing interoperability with some legacy components through use of Message Oriented Middleware (MOM) and CORBA.

<u>Data Sharing / Message Patterns</u> Successfully integrating messages and data across a wide community demands standards of data modeling and reference models. In the process of separating data from source systems a common mechanism to reconciling data definitions across sources essentially means an agreement on understanding.

Using existing metadata and data tagging models, it is possible to develop and share a common understanding of a single data element. When applied universally, this approach can lead to "Smart Data". [15] A metadata repository can serve as the single reference point for

[11] Webster, B.F., <u>Pitfalls of Object-Oriented Development</u>, M&T Books, New York, 1995, (p. 6).
[12] Technical Paper: Pritchett,WW *"An Object-Oriented Metrics Suite for Ada 95*" – DCS Corporation, 2001
[13] Technical Paper: Pritchett, W, and Landry, HC, *Interoperable Heterogeneous Data Access with CORBA and Ada 95*" – October 1998 – Fairfax, VA, Landry – DISA Center for Standards / JIEO / JEBE).).
[14] White paper: *"Global Combat Support System – Air Force"* – April 2002, (pg 2-3)
[15] Jackson,J. "*Taxonomy's not just design, it's an art"* – Government Computer News, Vol 23 #3, Feb, 9 2004, Interview with Michael C. Daconta, author of <u>The Semantic Web</u>.

maintaining rules about data services and data service requests and responses. This makes an NCC framework highly adaptive and responsive to changing environments.

Semantic Web Initiatives As metadata travels with the data element it provides a description of the internal data formats of the originating application. This "machine readable" model, however, does only part of the job – leaving a fundamental problem when one data consuming service (or application) potentially unable to translate the metadata the same way the service provider understands it. The W3C user community has since superceded the metadata model with the "W3C Semantic Web" project aimed at delivering a solution for dynamic discovery of data meaning. [16]

The W3C consortium has also supported efforts to define and adopt a common framework that allows data to be shared among any community. The collaborative known as the "Resource Description Framework" (RDF) establishes conventions for naming URLs and XML syntax. "RDF is based on the idea of identifying things using Web identifiers (called *Uniform Resource Identifiers*, or *URIs*), and describing resources as properties and property values. This enables RDF to represent simple statements about resources as a *graph* of nodes and arcs representing the resources, and their properties and values."[17]

Semantic Interpretation for Speech: Recent efforts have also been shifted to the ability to apply semantic interpretation to understanding content available in spoken format, "State Chart XML" (SCXML). A recent specification document by the W3C identifies an approach to apply grammar rules as a method for extracting meaning from speech recognition. This document defines both syntax and semantics of tag content for output as serialized XML.[18] While immature, this technology model could have significant impact on NCC services designed to update situational awareness input.

Adopting a Common "Knowledge Registry" Several years ago, the Department of Defense developed an ontology that would provide "syntactic interoperability". This model has two components 1) a single "knowledge registry" 2) a scheme for federated data sources.

The former used XML standards to create a "Virtual Knowledge Base" that served as a single knowledge registry accessible across the enterprise. When data originating from the federated sources was matched against the common registry, the information delivers relevant knowledge to the user community. It is possible to use the same approach to create a "semantic bridge" in cases where translation of metadata differs.

Data Sharing Bridge – Managed Content The notion of "semantic bridging" is a critical technology theme for an NCC architecture framework, since it drives to the essence of data exchange with "understandable" qualities. In effect, this accomplishment makes the difference between "data sharing" and "content management".

Some variations of this theme have been developed as a type of interface adapter for data consuming applications. This design is known as the "Metadata Adapter" or "Design-Time

[16] Manes, A. Web Services; A Manager's Guide, Addison Wesley, Boston, MA, 2003 (pg 143)
[17] Manola,F, Miller, E, – "Resource Description Framework (RDF) – Primer", W3C – 2004; Introduction
[18] W3C Specification Document: "State Chart XML (SCXML): State Machine Notion for Control Abstraction – Working Draft – January 24, 2006 (available at www.w3c.org)

Adapter".[19] The solution calls for the adapter to extract the metadata from the inbound data element, and use it to configure another "Message Translator". The translator step works as a bridge between applications. Similar approaches have been engineered into middleware for message brokers for years. Many commercial businesses specialize in these solutions including IBM MQ Series and BEA's Tuxedo products.

It is encouraging that the public sector is often the source of new enabling technology models for services that can benefit the mission of the NCC. The examples following drawn from OASD (NII)'s Horizontal Fusion initiative are representative of some early adopter initiatives that may contribute to the initial NCC architecture framework.

Federated Search: The Federated Search service is a knowledge discovery framework that provides authorized users and organizations on the network with the ability to search a vast array of indexed, non-indexed, structured, and unstructured data using a single point of entry. There are two major web services that make this possible, the Registration Web Service (RWS) and the Search Web Service (SWS). NCC will primarily use the Search Web Service to access existing intelligence information already existing in the Horizontal Fusion collateral space. The use of Federated Search will provide enhanced data discovery and its components for planning, resource discovery, and execution monitoring activities.

Shared Knowledge Distribution: NCC as Responsive and Innovative

For over 20 years, the evolving nature of information technology mirrors a changing idea of how "data" is understood and ultimately what it means to different consumers. In short, the notion of "data management" has eventually matured into the notion of "knowledge management". The section to follow explores technology models that enable distribution of knowledge to support decision making. Several examples of commercial solutions are shown in the figure 6.

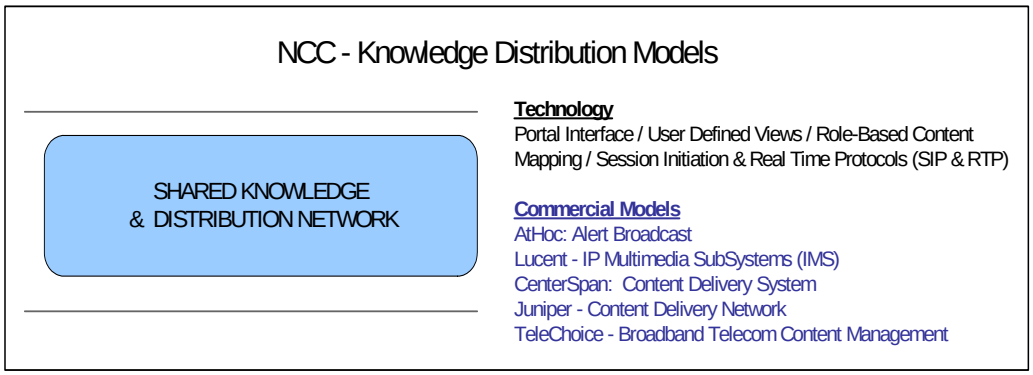

Figure 6. The NCC architecture framework will have a strategic dependence on methods applied to share information, content and ultimately, knowledge.

"The core Net-Centric environment emphases the data sharing that enables effective decisions."[20] Similarly, the core of a successful NCC design delivers the ability to distribute

[19] Hohpe,G., Woolf,B. – Enterprise Integration Patterns, Addison Wesley, Boston, MA, 2004 (pg 130).
[20] Steinbit, J. Department of Defense "*Net-Centric Data Strategy*", May 9, 2003 – Introduction (pg 3)

information in a way to allow users access to relevant knowledge. Such a framework will support situational awareness across unlimited communities, enable critical understanding of information and event patterns and finally, provide the means to take action. This is fundamental any public or private organization responsible for responding to urgent situations. In a word, this design supports a C2 system that is responsive. The NCC solution is to create web-based "portals" delivering a host of services and applications to anyone with a Web browser.

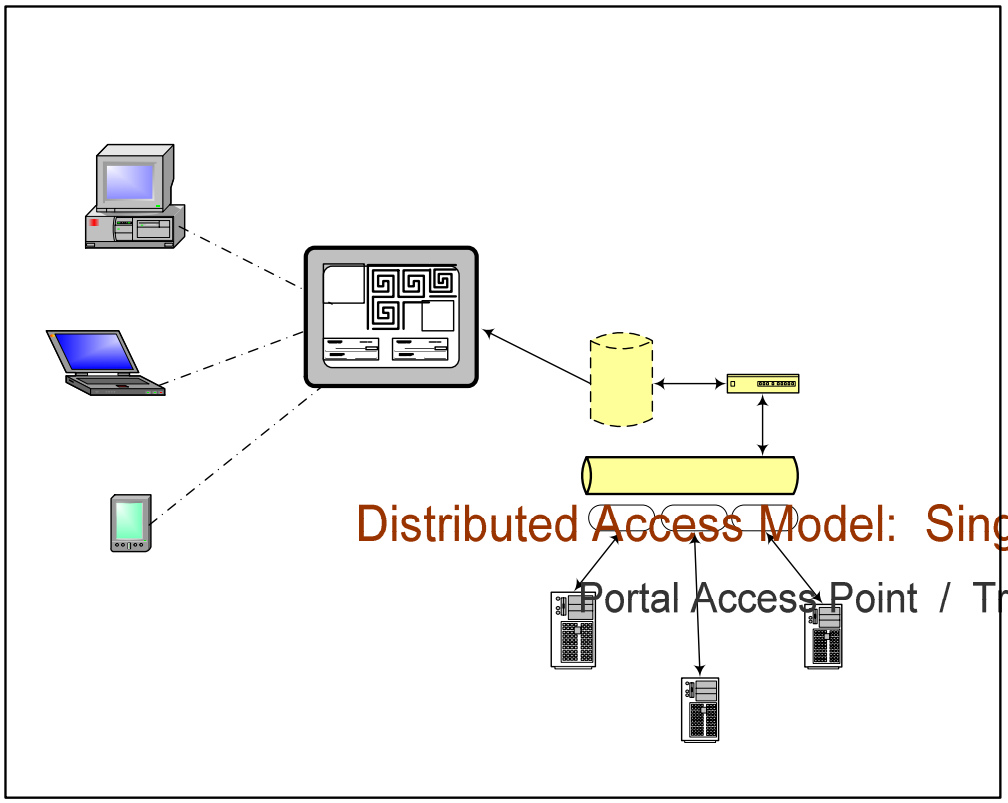

Figure 7. A key feature of the NCC architecture framework is to consolidate access to multiple data sources through the use of a common and customizable portal interface.

The universal NCC access portal will allow a user to perform a task on any device with an internet connection and a Web browser. An integrated national command and control applications and services suite will provide access to all functionality and data through open-component based set of routines, protocols, standards, and tools. It is this ubiquitous characteristic of the NCC architecture that will connect governing and responding agencies without geographical limitation.

Naturally, connection to the public can be augmented by traditional news media like radio, television, cable, and internet access. For example, the Department of Homeland Security has an initiative, Integrated Public Alert and Warning System (IPAWS) that integrates many of the same approaches.

NCC Access Portal

COI - #1
User Defined
Operational Picture

COI - # 2
User Defined
Operational Picture

COI - # 3
User Defined

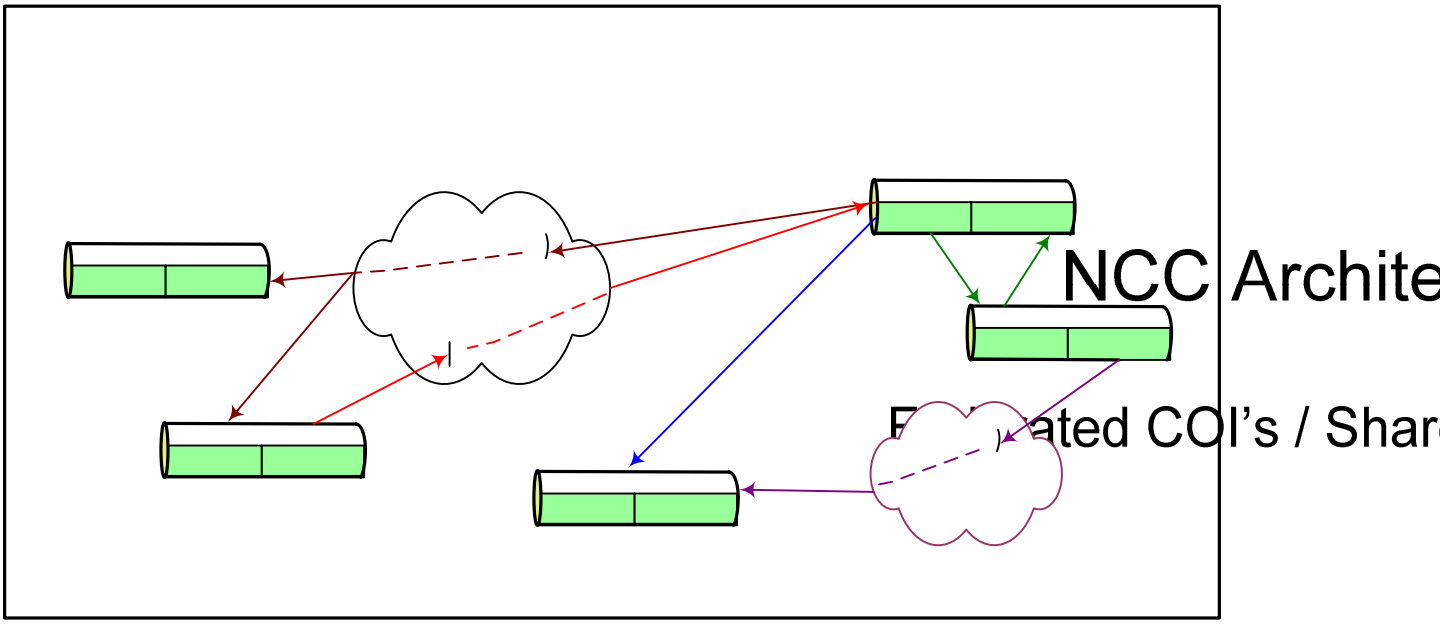

Figure 8. The intention of the NCC Architecture is to provide a means of interoperability and shared information across many communities of similar interests, in short, a "Federated Community of Interests".

Broadcast Alerts / Warnings" The mechanisms for "broadcast" messaging are not new, but when combined with more recent network hosting, domain name services (DNS) and publish-subscribe channels – the equivalent of "pop-up" ads are being used to deliver urgent information instantly to users working on the host network. The Air Force Air Education and Training Command has recently rolled out an "Early Warning" communications system that can send "…a message (that) will pop up on the hundreds or thousands of desktop computers being used on the unclassified networks throughout a base."[21]

Commercial solution providers are beginning to roll-out a "role-based" content mapping model that associates the content type with the consumer. One company, Athoc Inc., of California, markets their approach to deploying "role-based knowledge mapping tools"[22] with a knowledge gateway that will direct employees with specific business roles to content relevant to their productivity.

Geospatial Intelligence; The National Imagery and Mapping Agency (NIMA) initiative known as the National System for Geospatial Intelligence (NSGI) offers a set of services that provide critical data from combined "…multi-platform / multi-source exploitation including; airborne motion imagery cells."[23] Geospatial-intelligence (GEOINT) provides information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. In intelligence analysis and crisis response, GEOINT

[21] Wait, P. Early Warning – "*Taking a cure from eBay, Air Force adds a network component to base wide alert systems"* Article in Government Computer News – November 21, 2005.
[22] AtHoc, Inc., "Transform Knowledge into Action – and drive Multi-million dollar Productivity Gains" – 2005 - Case Study Marketing Paper
[23] Corporate Transformation Business Plan – FY04-05, National Imagery and Mapping Agency (pg. 8)

provides a means by which analysts, policymakers, war fighters, and first responders can visualize their environment.

GEOINT is an essential foundation for all-source intelligence users by providing a common reference point in space and time. With this ability, analysis is free to define a "common operating picture" (COP). Interestingly, the potential exists to develop a unique service to link Federated Search capabilities to NSGI to allow "streamlined delivery" of imagery products by having Federated Search discover and NSGI provide a "package" of NSGI mapping and imagery products based upon a GS Planner's "search objectives".

ISR Information Service (ISRIS): Another innovation to consolidate many data points to a single analytical view is the Multi-Sensor Aerospace-Ground Joint ISR Interoperability Coalition (MAJIIC) initiative. Here, the MAJIIC ISR Information Service (ISRIS) links airborne ISR assets (manned and unmanned) to the HF shared workspace. Near real-time ISR sensor data and platform mission data is discoverable via the Federated Search interface. These services include visualization features, ability to create a "user defined operational picture" (UDOP), live video mission feeds (or archived) from Predator UAV.

Environmental Visualization Information Service (EVIS): A remarkably responsive capability supporting situational awareness is available from this National Oceanic and Atmospheric Administration (NOAA) initiative. EVIS makes it possible to anticipate the potential affects of weather conditions on missions both planned and in progress. The EVIS capability combines intelligence, surveillance, and reconnaissance information together with high resolution metrological and oceanographic input for a forecaster to analyze. The basic services include analysis (including stoplight summaries, overlay images, and weather data) and Federated Search links. In short, this innovation consolidates data to create customized views necessary for mission planning.

DoD Portable Access Models Existing technologies have been applied in many DoD projects to quickly set up portable communication hubs in the field that can serve as distributed entry points into the broader information environment. Leveraging technologies like wireless mesh networks, cellular-based data technologies and others can lead to a NCC distributed network that supports a larger geographic area of first responders. These rapidly deployable networks can bridge a gap by providing the medium for key organizations and leaders to coordinate situation awareness and decisive actions. Although more work remains on integrating the means for effective information assurance, the technology model is both responsive and an innovative model for an NCC deployment architecture.

NCC Success Model: Trusted Environment

All this is occurring among the expanding community of internet-worked enterprises. In fact, the familiar boundaries of software applications, enterprise resource modules and networking typology are dissolving, yet interoperability depends on the open standards for IP protocols that support a converged network design.

This has a profound meaning for how the NCC architecture approaches security design. The ability to deliver the range of "Trusted Environment" services implicit in the NCC mission

must incorporate a kind of "global security" that results from innovations managing network infrastructure, access authentication, highly available operations, and information assurance.

These all describe the type of innovations that are necessary for transformation. The essential concept of the NCC "Trusted Environment" is to separate distinct security domains in a way that will support information assurance and user authentication.

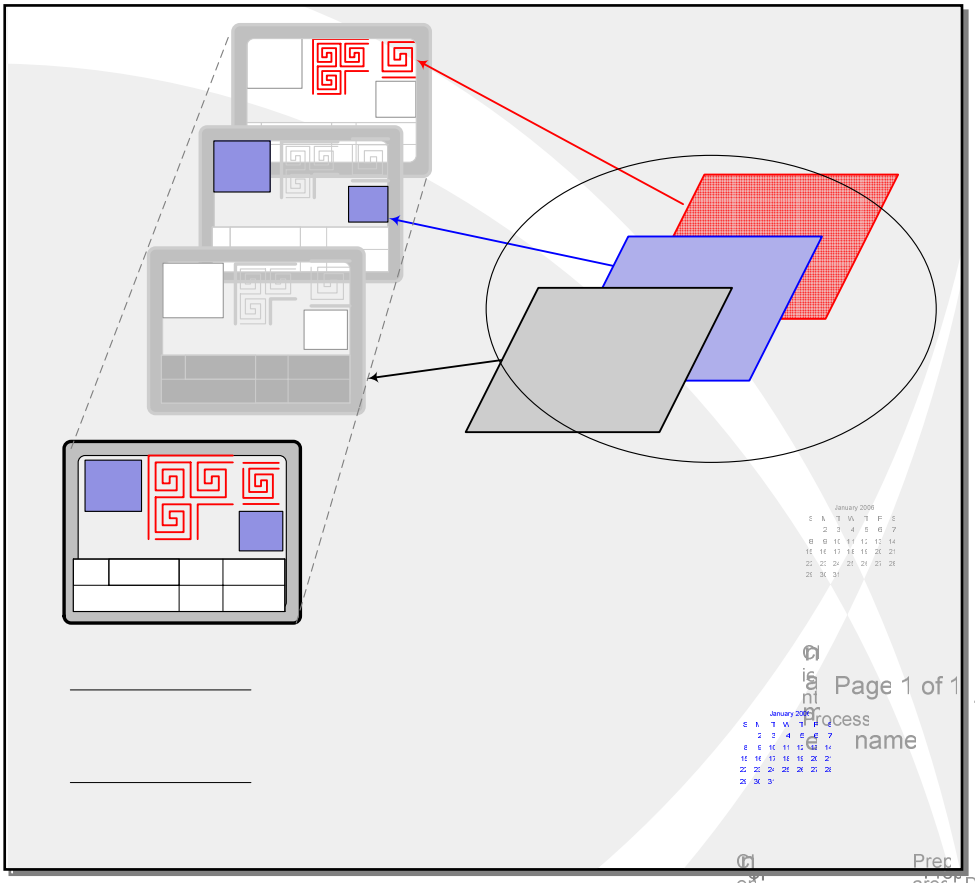

Figure 9. The NCC "Trusted Environment" will control security domains while managing a seamless user interface that appears seamless with respect to users access and authenticity.

Experimentation and discovery are the precursors of what some call "disruptive innovation" and like the paradox of competitor-partners in the public sector, many of "...the best ideas have come from competitors or adversaries."[24] This is one reason behind the merger of AT&T and SBC, Nextel with Sprint and Verizon with MCI. All these private sector examples of partnerships forged in search of innovations in communications technology – many will surly lead to solutions of information assurance and shared trusted spaces.

Likewise, competitors are meeting on common ground to establish standards that support the "next generation of converged network services". For example, two earlier protocol standards for IP services Session Initiation Protocol (SIP) and Real Time Protocol (RTP)

[24] Alberts, D., Hayes, R., Campaigns of Experimentation – CCRP publication, 2005 (p 45)

were initially intended for the IP core network architecture, although now they are viewed as enabling models for voice (VoIP), data and video network architecture as well. [25].

What has been termed the "converged network services" by Lucent Technologies, confronts new security and authentication controls for IP Multimedia Subsystem (IMS). The IMS architecture uses new standards by providing "trusted" interactions and "Call Detail Records (CDR's)". These ensure wireless and wire line networks can access one another.

The recent merger of AT&T and SBC represents a new force to pioneer technology in extended IP services over a wide reaching network. For example, almost a year ago AT&T had begun work on an "enhanced IP video conferencing service that would allow automatic audio to text translation. This capability would allow for users to search the archives of conferences for a specific point of interest by key word. [26]

Users at all levels must have the ability to add information, gain access to and share critical information, coordinate efforts, and provide updates to the changing conditions of a situation. The NCC will provide both a "trusted information environment" and ensure the ability to execute critical functions across the full range of threats from local and regional incidents to those of national significance. Multi-level security systems and cross-security enclave information sharing (from low to high, and from high to low where security, sanitization, and need-to-know permits) will be a key to the NCC development.

Secure information within critical state, local, and non-governmental networks would remain accessible to other secure networks (across either the Internet or Grid) through use of additional commercial encryption technologies. It will be available for operations in a day-to-day or crisis situation. An internet security approach might incorporate typical commercial encryption security and the NCC information. Integration with existing Net-Centric Enterprise Services (NCES) Security Mediation Services may be added to define a security domain.[27]

<u>DMZ Model – DISA Initiative:</u> Over a year ago, a familiar concept in network security, the "demilitarized zone" (DMZ), was enhanced by DISA Computing Services Systems Implementation Division to incorporate a full suite of security management measures. The "Concept of Operations" document for "DoD Internet Web Demilitarized Zone" describes the type of aggressive approach that will benefit NCC.[28]

NCC Success Model: "Organic Growth"

The NCC architecture framework will encourage users to become engaged with experimentation and future development. The expectation is that these mechanisms will fuel continued growth while expanding the core interests of the user community. As more commercial ventures employ web services to be profitable, they have discovered users willing to collaborate on new ideas to use existing services. Typically, e-businesses will sponsor sites offering access to services available for experimentation downloaded as a "kit"

[25] White paper: "Next Generation Communications Networks" – Lucent Technologies – January 2006.
[26] Pallatto, J. "*SBC Merger Won't Derail AT&T Plans*" – Article in "E-Week" – March 9, 2005
[27] Maskalenko,K. "*NCES Mediation Services*" Presentation – FGM Inc. October 19, 2005
[28] "DoD Internet Web Demilitarized Zone - Concept of Operations" – DISA, v 2.0, Aug, 28, 2004.

for off-line development. In some cases, a shared "test site" is available to perform some "beta" testing for innovative blended services or "mash-ups".

Amazon.com – offers a free downloadable kit (although a fee is required for use with purchases), more than 50,000 users have registered, paid the fee and are now creating hundreds of virtual storefronts for Amizon.com and other merchandise.

Google.com A free kit is available to download and is free for certain services.

eBay.com Offers a kit available for a fee and charges a "per-transaction" fee for its use. E-Bay has claimed that their top 50 affiliates (that is, users of the Web services API's) were earning $1 million a year in commissions.[29]

The continued growth of experimentation may be coordinated by other members of a community. For example those using Google services to improve their own similar search engine tools have organized the Search Engine Optimization communities or "SEOmoz" to provide a forum for shared experiences and ideas towards increasing visibility of Google searches to their sites. By providing access to a number of Google web services and unique API's, the development cycle of new services is greatly shortened.

Another example of collaborative development is known as "Wikis", essentially a content management system used for collaborative work processes. A "Wikis sandbox" is the established for creating dynamic web services, web content (in this case) that can be triggered to CGI scripts to dynamically generate HTML pages on a web server.

This type of creativity is at the heart of organic growth. Rich Karpinskik, editor of Network Computing, believes this to be a key of new applications, "Although IT departments may initially be reluctant to bring apps like Wikis" into the enterprise, eventually demand for such easy-to-use yet powerful apps will drive them… (and) make it easier for companies to bring in a best-of-breed Wiki application that will deliver real value quickly." [30]

NCC Success Model: Certification

Establishment of virtual federated lab for development of interoperable information and services in closed Internet environment is critical to ensure that remote entities and cross-department groups are integrating and leveraging one-another's efforts and using shared and common processes. The federated lab will allow sources of information and services an environment in which to experiment and develop solutions that will expose their services and data in accordance with service oriented architecture principles.

The federated lab will also help ensure that developers are applying the appropriate standards and that interoperable information and services are achieved. Information and services graduating from the test-bed will emerge "standards compliant" for NCC.

[29] Newcomer, E., Lomow, G., Understanding SOA with Web Services, Addison Wesley, Upper Saddle River, NJ, 2005 (pg 279).
[30] Karpinski,R., "The "Google-ization" of IT – The Next Big Wave of Change: Thanks to Google" – Network Computing – November 16, 2005

Finally a certification test cycle prior to deployment will assure the initial NCC system is able to meet functional requirements. Test scenarios to be considered might include; (1) hurricane Katrina, (2) the 9-11 attacks, (3) EMP attacks, (4) terrorism involving conventional weapons, (5) ground-based nuclear weapons detonations, (7) bio-weapons attacks, (8) chemical terrorism attacks, (9) solar tsunamis, (10) coastal tsunamis, (11) coordinated cyber attacks, (12) avian influenza, (13) a major New Madrid earthquake on the scale of the early 1800's occurrence, and (14) terrorism involving high power microwaves.

Conclusion

Advances in enterprise integration techniques and the development of transport protocols that enable information sharing have together, encouraged building applications to common standards and leveraging the flexibility of open system architectures. These conditions reflect the same spirit with which the internet development model has adopted, a willingness to engineer systems based on common standards and open systems.

If integration methods have become the means, then interoperability has become end. Interoperable services are quickly becoming the "value proposition available across an extended framework of networks. At the core of emerging "enabling technology models" is the capability to converge networks across a common framework.

Compelling motivators are driving both private and public organizations to work together. Keys of success and indeed, even survivability, will soon only be available through a common architecture framework that develops a converged network. The ability to deploy solutions that answer real business and public policy are now found among open systems and no longer in the realm of proprietary solutions.

APPENDIX

1. AUTHORITIES AND REFERENCES

STATUTES AND REGULATIONS.

1. The Defense Production Act of 1950, 50 App. U.S.C. 2061-2171, as amended through P.L. 106-363, October 27, 2000.
2. The Defense against Weapons of Mass Destruction Act of 1996 (Title XIV of the National Defense Authorization Act for Fiscal Year 1997).
3. The Robert T. Stafford Disaster Relief and Emergency Assistance Act, 42 U.S.C. 5121-5206, as amended through P.L. 106-390, October 30, 2000.
4. The Homeland Security Act of 2002, Public Law 107-296, dated November 25, 2002.

EXECUTIVE ORDERS.

1. Executive Order 12148, *Federal Emergency Management,* dated July 20, 1979, as amended by Executive Order 13286.
2. Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions,* dated April 3, 1984, as amended by Executive Order 13286.
3. Executive Order 12656, *Assignment of Emergency Preparedness Responsibilities,* dated November 18, 1988, as amended by Executive Orders 13074, 13228, and 13286.
4. Executive Order 13286, *Amendment of Executive Orders, and Other Actions, in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security,* dated February 28, 2003.

PRESIDENTIAL DIRECTIVES.

1. National Security Directive 42, *National Policy for the Security of National Security Telecommunications and Information Systems,* dated July 5, 1990.
2. Presidential Decision Directive 62, *Protection against Unconventional Threats to the Homeland and Americans Overseas,* dated May 22, 1998.
3. Presidential Decision Directive 67, *Enduring Constitutional Government and Continuity of Government Operations,* dated October 21, 1998.
4. National Security Presidential Directive/NSPD 1, *Organization of the National Security Council System*, dated February 13, 2001.
5. National Security Presidential Directive-4
6. National Security Presidential Directive-14
7. National Security Presidential Directive/NSPD-28, *United States Nuclear Weapons Command and Control, Safety, and Security*, dated June 20, 2003.
8. Homeland Security Presidential Directive 1, *Organization and Operations of the Homeland Security Council,* dated October 29, 2001.
9. Homeland Security Presidential Directive 3, *Homeland Security Advisory System*, dated March 11, 2002, as amended by Homeland Security Presidential Directive 5.

10. Homeland Security Presidential Directive 4, *National Strategy to Combat Weapons of Mass Destruction*, dated December 2002.
11. Homeland Security Presidential Directive 5, *Management of Domestic Incidents*, dated February 28, 2003.
12. Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*, dated December 17, 2003.
13. Homeland Security Presidential Directive 8, *National Preparedness*, dated December 17, 2003.

OTHER GUIDANCE.

1. Federal Preparedness Circular 65, *Federal Executive Branch Continuity of Operations (COOP),* dated June 15, 2004.
2. *National Response Plan,* dated December 2004.
3. Memorandum from: Frances Fragos Townsend, Assistant to the President for Homeland Security; Subject: Continuity Policy/Department and Agency Essential Functions, dated January 10, 2005.
4. Memorandum from: Joshua B. Bolten, Director, Office of Management and Budget; Subject: Regulation on Maintaining Telecommunication Services During a Crisis or Emergency in Federally-owned Buildings, dated June 30, 2005.