12th ICCRTS

"Adapting C2 to the 21st Century"

Suggested Topics:
C2 Concepts, Theory, and Policy
Networks and Networking
Metrics and Assessment
C2 Technologies and Systems

THE TROUBLE WITH C2 ARCHITECTURES

Dr. Raymond J. Curts, CDR, USN (Ret.)*
Strategic Consulting, Inc.
5821 Hannora Lane
Fairfax Station, VA 22039-1428
voice: (703) 425-6982 / fax: (775) 254-4248
rcurts@ispwest.com

Dr. Douglas E. Campbell, LCDR, USNR-R (Ret.)
Syneca Research Group, Inc.
P.O. Box 2381
Fairfax, VA 22031
voice/fax: (703) 876-0935
email: dcamp@syneca.com

* Primary point of contact.

© Copyright 2007, Curts & Campbell

12th International
Command & Control Research and Technology Symposium

THE TROUBLE WITH C2 ARCHITECTURES

Dr. Raymond J. Curts, CDR, USN (Ret.)*
Strategic Consulting, Inc.
5821 Hannora Lane
Fairfax Station, VA 22039-1428
voice: (703) 425-6982 / fax: (775) 254-4248
rcurts@ispwest.com

Dr. Douglas E. Campbell, LCDR, USNR-R (Ret.)
Syneca Research Group, Inc.
P.O. Box 2381
Fairfax, VA 22031
voice/fax: (703) 876-0935
email: dcamp@syneca.com

Abstract

Architectures and their processes have been popular for some time in both government and industry to design and understand the enterprise, usually the Information Technology (IT) and Decision Making infrastructure of the enterprise. Over the years there have been a very large number of architectural efforts undertaken. In addition, nearly every major government department and agency (and many industry groups) have created their own processes, procedures, and frameworks for the development and standardization of architectural artifacts - all with limited results. In this paper the authors first investigate several of these previous efforts, their successes and failures, and the most apparent reasons for those outcomes. We then touch upon some current architectural efforts and explain why most are doomed to failure if they proceed on their current paths. The paper culminates in suggestions for conducting future architecture efforts in order to apply more useful, repeatable, enduring results toward adapting C2 to the 21st century.

* Primary point of contact.

© Copyright 2007, Curts & Campbell

THE TROUBLE WITH C2 ARCHITECTURES

Dr. Raymond J. Curts, CDR, USN (Ret.)
Dr. Douglas E. Campbell, LCDR, USNR-R (Ret.)

1.0 BACKGROUND / INTRODUCTION

Over the years, several attempts have been made to "architect" various aspects of the Armed Services, other government departments and agencies, and commercial entities. Indeed, the concept is not new. Though described by a variety of titles, the United States military has been in the process of composing "architectures" for many years. The actual process of "architecting" forces has been going on since the inception of armies and navies; in the case of the United States, that dates back to 1775. When the country was young and the militia small, the process was relatively easily handled by a small staff (in some cases one person) with paper, pen, and a firm grasp of military and/or naval tactics, seamanship, etc. As the force grew larger, however, more men, paper, pens, expertise (in both depth and breadth), and time were required to keep track of the current forces as well as to stay abreast of emergent technologies. To compound the problem, the military was split into several Brigades and Fleets, which were further divided into Battle Forces and Task Forces, and other, smaller combat units. It took many years of evolution for the job to eventually become overwhelming and it continues to get more and more complex.

In the late 1990s, the Office of then Assistant Secretary of Defense for Command, Control, Communications and Intelligence (OASD(C^3I))[1] commissioned a number of studies to review the status of architectures within the Department of Defense (DoD). The findings were reported to a variety of offices and agencies within OASD(C^3I), all of which had been designated to support various aspects of architecture development for DoD as recommended in a Defense Science Board Summer Study on Global Surveillance [DSBGS, 1993]. Many of these architectures focused on Command and Control (C2) systems which have been articulated in the government arena as those that "can coordinate widely dispersed units, receive accurate feedback, and execute more demanding, higher precision requirements in fast moving operations" [DISA, 2003].

Since that time, world events such as Hurricane Katrina and terrorist attacks of 11 September 2001 in the United States, subway bombings in Great Britain and a number of other incidents throughout the world continue to demonstrate the need for better information flow throughout the enterprise to include federal, state, local and tribal governments, and first responders, not to mention the military and the intelligence community.

Also in the late 1990s, the primary DoD guidance on architectures was the Technical Architecture Framework for Information Management (TAFIM), developed by the Defense Information Systems Agency (DISA). The TAFIM focused on the evolution of Department of Defense (DoD) systems, including sustaining base, strategic, and tactical systems, as well as interfaces to weapon systems. Application of the TAFIM reference model was required on most DoD systems [Paige, 1993]. TAFIM was a set of services, standards, design components, and

[1] Currently Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)).

© Copyright 2007, Curts & Campbell

configurations that were used in the design, implementation, and enhancement of information management system architectures. The intent was that the DoD infrastructure would have a common architecture that would, over time, be a fully flexible and interoperable enterprise. [TAFIM, 1994].

Since there were no commonly used approaches for architecture development and use within DoD, the Commanders In Chief (CINCs), the military Services, and DoD agencies were increasingly developing and using architectures to support a variety of objectives, such as visualizing and defining operational and technical concepts, identifying operational requirements, assessing areas for process improvement, guiding systems development and implementation, and improving interoperability. Many different constructs were used to build and portray architectures. TAFIM did not fully specify components and component connections [Clements, 1996] nor did it dictate the specific components for implementation (no reference model prescribes implementation solutions). Systems built using TAFIM were criticized by RAdm. John Gauss, then the Interoperability Chief at DISA, when speaking on systems in the field in Bosnia: "We have built a bunch of state-of-the-art, open-systems, TAFIM-compliant stove-pipes." [Temin, 1996].

There were excellent initiatives, such as Air Force C4I Horizon, Army Knowledge Enterprise Architecture, and Navy Copernicus. These were forward-thinking initiatives but generally they were not connected. On a schematic, the interface was usually a cloud (almost an afterthought), euphemistically labeled "a miracle happens here." At the DoD level there were various architecture forums, such as the Architecture Methodology Working Group, the Architecture and Integration Council, and the Intelligence Systems Board, but they were also not readily coupled.

The TAFIM's SBA Methodology described a process to develop and achieve an integrated information technology architecture that some DoD organizations chose to use. Likewise, several of the Services, and some of the commands and agencies established processes for developing, presenting, and managing architectures. The processes and products varied according to the organization, and some were more mature than others. This multi-track approach to the Command, Control, Communications, Computers, And Intelligence (C4I) architectural world often yielded stovepiped, inconsistent, non-interoperable C4I architectures. The community was unable to fully leverage across various architectures to develop a seamless, integrated C4ISR environment [CISA, 1996].

If a truly joint and interoperable enterprise is ever to be achieved, the concept of a single unifying construct, however imperfect or incomplete, must receive support at the highest levels of DoD and other government agencies. Although the plan proposed by the authors is, no doubt, imperfect, it is, at least, a start and is offered as a first step toward a government-wide interoperable C4I architecture. The missing ingredient seems to be a single unifying construct to lay the foundation for multiple architectures and tie them together. Probably the most glaring deficiency lies in exactly the location that is causing the most dialogue and the need for architectures to begin with — the interface points. Almost all architectures designate some small set of peripheral nodes as the "connection to" the systems, structures, architectures of other agencies. As one might expect, these are the nodes that are given the least attention (because they are generally outside the realm of the agency producing the architecture) and, therefore, are

© Copyright 2007, Curts & Campbell

the least well-defined. Though composed of innumerable components / segments the enterprise must function as an integrated, interoperable whole (Figure 1). What we have set aside as being too complicated to architect, the primary reasons for architectures in the first place, has come back to bite us.

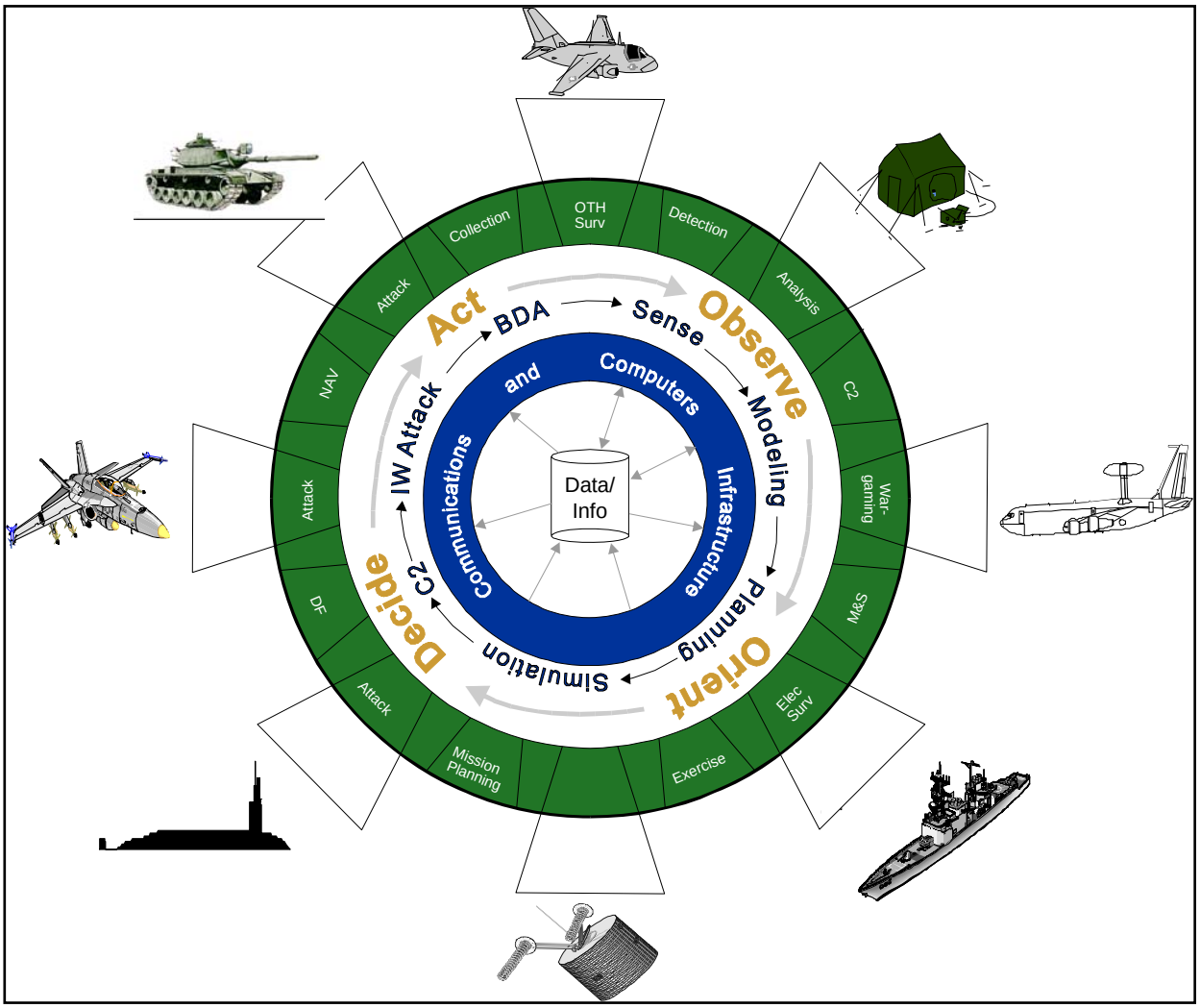

Figure 1: The Information Sharing Requirement

Virtually every mission, operation, platform, system, and individual is heavily dependent upon timely, accurate, reliable data and the infrastructure through which it moves. Consequently, that data and the infrastructure must be connected and interoperable so that the information can be shared, protected (Figure 1's outermost, green ring), trusted, secure and assured. Data is at the center of everything. It is shared among those who need it via the Communications and Computers infrastructure (innermost, blue ring). Whether we talk about the OODA Loop[2], MAPE[3], Battle Timeline[4], or the Sensor to Shooter Cycle[5], there are a number of functions that are routinely performed.

[2] Observe, Orient, Decide, Act (Col. John Boyd, USAF) [Boyd, 1986]
[3] Monitor, Analyze, Plan, and Execute (Air Force Doctrine Center)

© Copyright 2007, Curts & Campbell

- We sense the environment and store the data that we collect.
- We use that data to construct models and simulations of the known environment and plan our actions.
- Commanders employ this wealth of information, and the infrastructure upon which it flows, to Command & Control (C2) their forces deploying and directing them as necessary in both peaceful and hostile actions.
- And, finally, we conduct Battle Damage (after action) Assessment (BDA) to determine what affect we've had and how the environment has changed - which brings us back to sensing the environment.

This cycle, of course, is recursive and in any actual engagement there are a number of people performing each of these functions all at the same time. The trick is to do it better, quicker and more reliably than the adversary. Or, get "inside his OODA Loop" as the saying goes. Most agree that this is what needs to happen yet we seem to be having a good deal of difficulty making the process seamless, timely, accurate and reliable.

Still, buzz words like "jointness," "interoperability," and "integrated" continue to be bandied about every time United States military forces, intelligence organizations and disaster recovery agencies engage in any newsworthy operation. Why? Because in each successive engagement we find another instance in which our respondents have been unable to adequately plan, communicate and/or coordinate multi-unit activities. Take, for example, the Air Force Contingency Tactical Air Planning System (CTAPS)[6].

During Operation Desert Storm, the Navy was unable to share mission planning data compiled in CTAPS. During that conflict, air plans had to be hand carried to the aircraft carriers in hard copy. Often the issues are much longer standing. In all cases, however, some service, agency or organization has and is actively using some system (usually a command and control, intelligence or other information sharing system) that will not connect to, interface with or in some fashion interoperate with other participating services, agencies and organizations.

The situation has been studied at a variety of levels—from the Office of the Science and Technology Policy (OSTP) in The White House to individual state, local and tribal responders and combat units. So why then, in this age of complex, automated information systems, have we failed to achieve total connectivity and interoperability [Curts, 2006]?

---

[4] Typically something similar to: planning; surveillance / reconnaissance; acquisition; targeting; weapons direction and guidance; homing and fuzing; and post-timeline assessment

[5] Usually defined as the time-critical process by which targets are detected, identified, classified and engaged.

[6] CTAPS generates USAF Air plans which were not compatible with USN systems.

© Copyright 2007, Curts & Campbell

2.0 EXAMPLES OF FAILED CONNECTIVITY / INTEROPERABILITY

Other examples of where we failed to achieve such connectivity and interoperability include Grenada, Kosovo, Operation Iraqi Freedom, 9/11 and Hurricane Katrina. Briefly:

2.1 Grenada. The short-notice decision in 1983 to deploy joint forces to Grenada, made in response to a perceived crisis, left each military service no time to develop mechanisms for communicating with the other services. The joint forces, constructed on an ad hoc basis, faced the need to achieve interoperability essentially on the fly. Reports that appeared in the media almost as soon as the mission ended, and subsequent congressional testimony by military leaders, showed that the U.S. forces largely failed to do so. Although many of the specific incidents reported and the remedies suggested to prevent them from recurring in the future have never been confirmed in unclassified official literature, some unofficial accounts acknowledged the problems [Snyder, 1993]:

> *"The final challenge to invading forces was the lack of a fully integrated, interoperable communications system … it was reported that one member of the invasion force placed a long distance, commercial telephone call to Fort Bragg, N.C., to obtain C-130 gunship support for his unit which was under fire.… Commenting overall on the issue of interoperability, Admiral Metcalf [the CINC of Atlantic Command and the overall commander for the operation], wrote, 'In Grenada we did not have interoperability with the Army and the Air Force, even though we had been assured at the outset that we did.'" [Anno, 1988]*

2.2 Operation Allied Force, Kosovo. One lesson of Kosovo Operation Allied Force in 1999 was that the intelligence community did not have enough capability to analyze the images and the other raw material that was collected [Pike, 2000]. The Kosovo mission also offered examples of shortfalls in allied interoperability under combat conditions. In a joint statement to the Senate Armed Services Hearing on Kosovo, the senior leadership of both the U.S. and North Atlantic Treaty Organization (NATO) forces identified interoperability as an impediment among the allied troops. General Wesley Clark, NATO Supreme Commander, Admiral James Ellis, Commander of Allied Forces–Southern Europe, and Lieutenant General Michael Short, Commander of Allied Forces–Central Europe, had this to say:

> *"Finally, Operation Allied Force illuminated the capability gaps between the U.S. military and our NATO allies…. These gaps impeded interoperability among Allied forces during the campaign…. Ultimately, NATO nations need to upgrade their militaries to ensure they remain compatible with U.S. Forces." [NATO, 1999]*

2.3 Operation Iraqi Freedom. Effective C4I systems were supposed to ensure that joint intelligence and total battlespace information awareness would be provided to the warfighter through the use of common Tactics, Techniques, and Procedures (TTPs). These systems were also intended to provide the warfighter with the flexibility to support any mission, at anytime, anywhere. In Operation Iraqi Freedom (OIF), C4I systems actually experienced significant faults while attempting to address these challenges. Admiral E. P. Giambastiani, Commander, U.S. Joint Forces Command, said it best:

© Copyright 2007, Curts & Campbell

> *"Where we fall short is when we're in a high-speed, fast-moving campaign, like this one was, where our forces are moving very rapidly. The ability to be able to do effects assessments or battle damage in a rapid fashion lacks (sic) seriously behind the movement of our forces." [Giambastiani, 2003]*

Methods for reviewing tactical aircraft Weapon System Video (WSV), for example, lacked the C4I systems and personnel expertise necessary to forward the WSV to the CENTCOM Joint Intelligence Center (JICCENT) in Tampa, FL, for timely analysis and use by commanders. The WSV often arrived for analysis at JICCENT eight to ten hours after the aircraft completed its mission. Once there, JICCENT lacked the requisite subject matter experts to quickly exploit the large number of WSV, thereby exacerbating the time delay of fused BDA reports. The exploitation, production, analysis, and dissemination processes were unresponsive to the operational speed of maneuver [Bradley, 2004].

2.4 9/11. One of the main issues raised during the first Association of Public Safety Communications Officials International (APCO) conference in 1935 was interoperability. Then it was called "inter-city communications," said APCO President Wanda McCarley [McKay, 2006], but was essentially the same thing -- only on a lesser scale. More than 70 years later, interoperability is still a hot topic.

Now it's defined as "the ability to share information via voice and data signals on demand, in real time, when needed and as authorized." What's changed since 1935 is the scope and depth of the problem. The inability to deal with it, despite decades-long efforts, remains. There are many incidents to reference in the last two decades, but 9/11 re-emphasized the problem's breadth and depth. So how much have we gained on the problem since 9/11?

"Relatively little," said Viktor Mayer-Schönberger, associate professor at Harvard University's John F. Kennedy School of Government. "Some regions and metropolitan areas have moved ahead, but in general, we are still in the stone age of interoperability. If a 9/11-like disaster would happen today, in most jurisdictions we would still have to use runners to communicate among first responders." [McKay, 2006]

2.5 Hurricane Katrina. The Associated Press reported that "Police and other emergency agencies responding to Hurricane Katrina were plagued by their inability to talk to one another on their radios within the same city, and across multiple cities and regions. Tight space on the radio spectrum, bureaucratic disagreements over how to resolve the problem, and the sheer number of local, state and federal agencies involved in disasters have all complicated the search for an answer. A project in San Diego illustrates the difficulty. It took only about 30 days to put in place the technology needed to improve communications. But it took nearly two years to get all the agencies—police, fire, federal officials and others—to agree to the plan." [Kerr, 2005]

So what is the underlying cause of this interoperability issue? Why can't the departments and agencies design, acquire and implement joint, interoperable systems? There are, no doubt, a plethora of issues; none of which are easily solvable. Many blame the procurement / acquisition system. Others think that congressional oversight of military, intelligence community and

© Copyright 2007, Curts & Campbell

related procurement is the root of the problem. At least one answer lies in requirements definition, requirements allocation and the procurement cycle itself. The process of defining what is needed, analyzing and applying alternative compromises born of conflicting requirements and budgetary constraints, and planning for a fully interoperable, joint enterprise is very complex, disjointed and is generally not amenable to cooperative development of fully interoperable systems. All of the services and many other government agencies have begun to investigate these issues. The results are generally titled "Master Plans" or "Architectures" although other terms such as "Vision," "Acquisition Strategy," "Roadmap" and "Portfolio Management Plan" have frequently been used.

In the authors' opinion the primary difficulty is that we have never found and implemented a suitably robust, consistent, automated, integrated architecture process that will allow us to capture required capabilities, compare them to existing capabilities, design, test and select acquisition alternatives, and develop the fully integrated, cost effective, interoperable systems that we need.

The authors examined what we believed to be the root cause of this and similar compatibility and commonality issues. The examples given in this paper are taken from the authors' personal experiences working with the architecture definition and development processes within the Navy, the Intelligence Community (IC), Department of Homeland Security (DHS), OSTP, Office of Management and Budget (OMB) and other government departments and agencies. Several other studies, however, have been conducted by and/or for numerous other services and agencies. Some of these other studies are referenced where appropriate.

3.0 SO, WHAT'S THE PROBLEM?

First, the timeliness of our decision processes is important (especially during conflict or catastrophe) which implies that the timeliness and quality of the information upon which we base those decisions are important. In order to provide timely, quality information we must have a fully interconnected, interoperable, reliable infrastructure which brings us back to a well defined architecture (Figure 2). An architecture is nothing more than an outline for how we build our system and what functionality it will have when it is done. And, we have known for years that a good architecture requires a structured, standardized, repeatable, development and acquisition methodology. And all of this is not worth much unless the architecture is actually implemented and operated by a strong, robust support organization.

According to Webster's II New Riverside University Dictionary the word "architecture" is defined as "... the art and science of designing and erecting ... a style and method of design and construction ... design or system perceived by humans ...." [Webster, 1984]. Similarly, JCS Pub 1-02 defines architecture as: "A framework or structure that portrays relationships among all the elements of the subject force, system, or activity." [CSC, 1995] There are numerous other definitions as well but for our purposes, the following will suffice:

> *Architecture*: "An organized framework consisting of principles, rules, conventions, and standards that serve to guide development and construction activities such that all

© Copyright 2007, Curts & Campbell

components of the intended structure will work together to satisfy the ultimate objective of the structure." [CIMPIM, 1993]

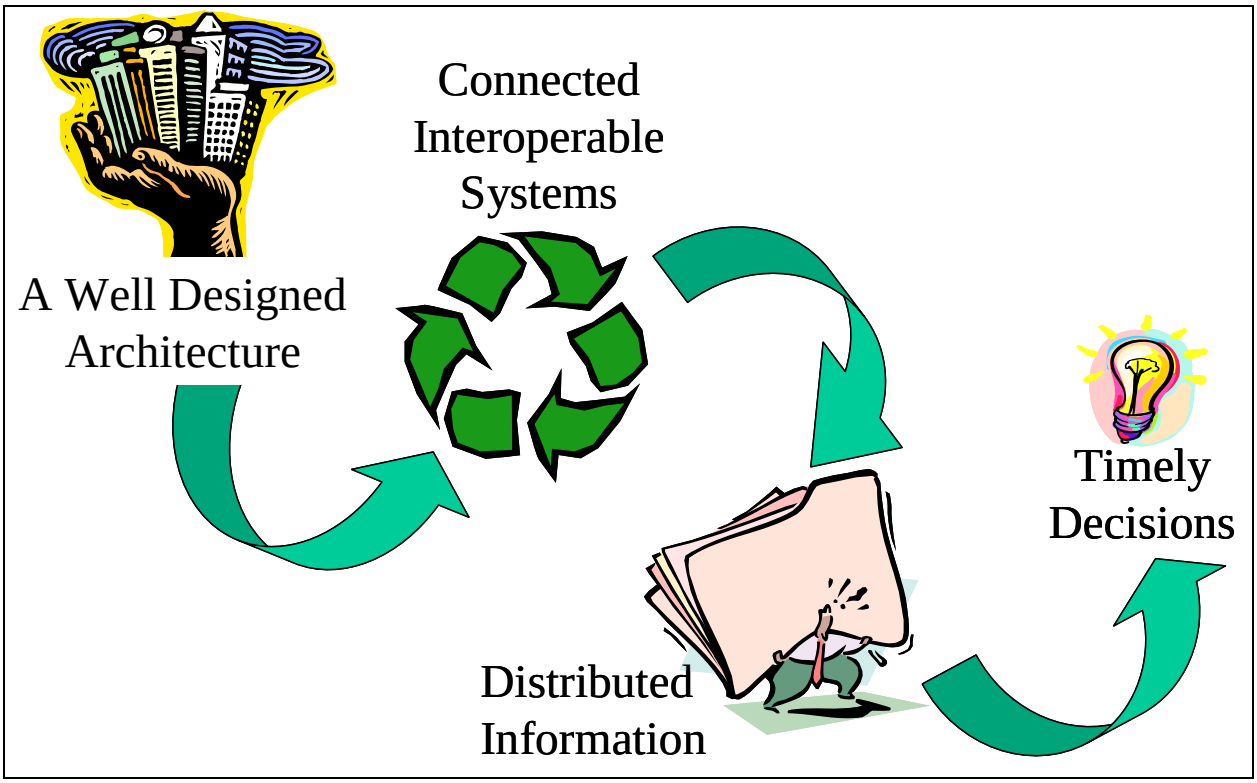

Figure 2: Architectures and Decision Making

Another important concept is Information Assurance (IA). *Information Assurance (IA)* is the ability to make the right information available to the right people, in the right place, at the right time with some reasonable expectation that it is timely, accurate, authentic, reliable and un-compromised. IA is more than just security. Given that definition, we can't get the information to the right guy at the right time (we can't do IA) unless our systems can exchange information (i.e., are interoperable), and we can't expect any reasonable degree of interoperability without a plan, a blueprint, an architecture – something that tells us where and how all the pieces fit together.

The ability to generate and move information has increased many thousands of times over the past 30 years. The services and other government agencies have all become much more reliant upon information technology. Unfortunately, the current capability to generate information far exceeds our ability to disseminate, control and use it effectively.

In a paper presented at the 1997 DoD Database Colloquium, James Mathwich made the case that the seamless flow of information is one of the most ambitious visions of information operations.

> *"And yet within the Department of Defense, database integration and information interoperability efforts are more often characterized as false-starts rather than successes."*

© Copyright 2007, Curts & Campbell

> *"Automation of information management cannot be done on a community-wide basis unless there exists a community-wide policy with sufficient detail so that it can be predictably executed in an automated tool…. The definition and management of the linkage between information and mission has in the past been lacking."* [Mathwick, 1997]

The Joint Interoperability Test Command (JITC) performs the joint interoperability test and certification mission as prescribed in joint staff instruction CJCSI 6212.01A [JITC, 1998]. From JITC we have this definition of ***interoperability***:

> *"The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces, and to use the services so exchanged to enable them to operate effectively together."*

In a briefing given to the Department of the Navy (DoN) Chief Information Officer (CIO) in February of 1999, the concern with interoperability issues was apparent. "Data efforts are uncoordinated and there is no process in being to fix the problem. Many C4I systems are incapable of sharing and exchanging data, an interoperability problem that could result in the possible 'loss of life, equipment or supplies'. To correct the problem requires both an information architecture and a repository of systems' databases." [Michaels, 1999] We have already shown that little has changed (e.g., OIF, 9/11, Katrina, etc.).

These seem to be relatively straightforward concepts. So we will repeat the questions: Why then is the process of identifying and developing architectures so difficult, costly and time consuming? And, why, despite years of research and millions of dollars spent investigating the issues, are we still struggling to:

- define what exactly constitutes an architecture,
- identify what types of architectures do and/or should exist,
- categorize architecture concepts, and
- develop a long-range plan for architecture development and maintenance?

Without a consolidated, coordinated, organized plan there is little chance of ever attaining the elusive goal of total interoperability.

Terminology changes from time to time and some previous "buzz" words have fallen from favor. The terms "capabilities" and "requirements," for example, have been over used and have acquired some confusing connotations over the years. But, for purposes of this discussion, the authors use the term "architecture, interoperability and information assurance" as defined above. Webster's definitions of requirements and capabilities seem perfectly adequate for our purposes [Webster, 1984]:

> *Requirement* – something needed; that which is required; a thing demanded or obligatory; a need or necessity. In architecture terms: functionality that is required in order to do

© Copyright 2007, Curts & Campbell

whatever it is we want / need to do. A requirement represents a needed functionality whether it currently exists or not.

Capability – potential for use; the quality of being capable; capacity; ability; qualities, abilities, features, etc., that can be used or developed; potential. An existing functionality. A capability represents a functionality that currently exists whether it is needed or not.

4.0 PREVIOUS EFFORTS

The ultimate goal of any planning process is, of course, to build a knowledge- and experience-base upon which to formulate decisions toward shaping the future design of organizations and information flow. This is more than just managing information. Planners must be able to organize and/or re-organize the components of a large, complex system so that it functions smoothly as an integrated whole. We must be able to manage, manipulate, and study the effort on a conceptual level so that it can be implemented on the physical level.

4.1 SPAWAR / CNO. In the mid-1980s, the Space and Naval Warfare Systems Command (SPAWAR) in conjunction with the Chief of Naval Operations (CNO) formulated an initiative to perform force warfare assessments under their Warfare Systems Architecture and Engineering (WSA&E) charter. As of June 1988 the Navy had budgeted $91.5 million for the WSA&E process in ever increasing yearly increments from Fiscal Year (FY) 87 through FY 94. The purpose of these assessments, like others conducted by a variety of services and agencies, was to perform both top-down and bottom-up analyses of platforms, weapon systems, and support systems in terms of their impact at the force level and effectiveness. The WSA&E process represents just one of the Navy's coordinated efforts to make tradeoffs across warfare mission areas in a structured, analytical way. The process was driven by the belief that the Navy's R&D and acquisition decision process was/is inundated by a proliferation of requirements and procurements that [WSA&E, 1988]:

(1) provide a fragmented approach to Battle Force Command and Control;
(2) indicate a lack of understanding of interoperability issues; and
(3) result in programming actions taken without a full understanding of their impact on other interrelated programs.

The goal then, is to integrate and coordinate these requirements into a framework where the force is viewed as a single warfighting system.

The Navy's plan, like many others, was well thought out and structured. Architectures were defined, at least by some, as the long-range goal, a blueprint for what was desired/expected in 10 to 20 years. In the interim, the service expressed its intermediate plans/goals in 5-10 year planning documents known as Master Plans. In the near term, of course, we had the well-established Program Objective Memorandum (POM) process, a five-year plan of budgeting and procurement.

© Copyright 2007, Curts & Campbell

Unfortunately, the funding for architecture development in the Navy dwindled to the point of virtual non-existence long before the process was complete. There are, no doubt many reasons for this demise but one of the most prominent was the fact that architectures take a good deal of time to develop and the developers argued that they could not provide many answers until they were very nearly finished. In fact, some would argue that architectures are never finished because they require continual update and enhancement to account for technological advances, program adjustments, congressional actions, and a host of other variables. Hence, the answers that architectures were expected to provide came slowly.

Architectures were originally developed, at least within DoD, to help program sponsors make informed, timely, accurate decisions in the seemingly never ending battle of the budget and perpetual change.

> *"Architectures provide a mechanism for understanding and managing complexity. The purpose of C4ISR architectures is to improve capabilities by enabling the quick synthesis of "go-to-war" requirements with sound investments leading to the rapid employment of improved operational capabilities, and enabling the efficient engineering of warrior systems." [CAF, 1997]*

Although this effort did provide valuable insight into the procurement process and the technological issues in many warfare mission areas, the process was never completed to the point where a true migration path could be identified and pursued.

4.2 SSC-Charleston. These WSA&E efforts were followed by a number of others. SPAWAR Systems Center Charleston (SSC-C) revived the architecture process in the 2003 – 2006 timeframe. They employ automated tools that significantly reduce the timeline and increase the usability of the data collected. Previous architecture efforts had generated a goodly number of documents and views, within DoD mostly artifacts prescribed by the DoD Architecture Framework (DoDAF). Despite the requirement for predefined views; charts, graphs, wiring diagrams, tables and other "pretty pictures" are NOT an architecture. At best they are a representation of an architecture at some point in time. Since architectures, especially information architectures, change almost daily, these representations became obsolete and marginally useful almost immediately. In addition, paper documents (text files, slides, etc.) such as are typical, do not capture the data behind the picture and are very laborious and marginally useful as decision aids. These products, therefore, became shelfware that fulfill a requirement (for each agency to "have" an architecture) but, beyond that, they have little use and are, in fact, little used. The work at SSC-C goes well beyond predefined artifacts and actually captures the data behind the pictures. This process, methodology and tools have been used to conduct the Navy's ForceNet assessment and, by most accounts, have been very successful.

4.3 Unified Command Structure (UCS). Superior information leading to shared awareness and, hence, superior decision-making has long been recognized as a force multiplier. The future of C2, as embodied in Network-Centric Warfare (NCW) demands the availability of a large number and variety of functional capabilities at all levels of command. C2, like all warfighting disciplines, must be tightly and seamlessly integrated to produce a common tactical picture, shared awareness, shared understanding, net-centricity, Agile C2 and a host of other objectives that we strive to achieve in our quest for "Perfect C2." We can no longer afford to develop

© Copyright 2007, Curts & Campbell

stove-piped systems, tools and architectures. Neither can we afford to start from scratch. Instead we must leverage the existing set of systems, programs, services, organizations and supporting infrastructures that form the basis upon which we can build. We do this via a repeatable, defendable, systems engineering process that "… optimizes total system performance and minimizes total ownership costs….." across the C2 Enterprise [Robinson, 2004].

The Unified Command Structure (UCS) provides overall governance, policy, guidance, processes and procedures for the conduct of integrated, enterprise-wide C2. The goal of Enterprise C2 (EC2) is a globally connected, fully integrated and interoperable collection of systems and services to support National / Strategic C2 and allow seamless interaction with Theater / Tactical C2 operations, i.e., a well planned, managed Portfolio. The EC2 effort provides the catalyst for a leap forward to net-centric C2 capabilities—a move that overtakes the current evolutionary approach toward modernizing defense capabilities to assure an adaptable, reconfigurable, full-spectrum C2 capability for warfighters and senior leaders operating within a collaborative information environment.

Timely decision-making depends upon our ability to collect and interpret relevant data better and faster than our adversaries which means that decision makers need a Shared Understanding / Awareness that closely approximates reality. We achieve this by defining our goal policies, processes, procedures and functional capabilities for the conduct of "Perfect C2," to support the optimization of our acquisition processes allowing a calculated, orderly migration toward achieving those capabilities through a robust methodology. Though there has always been recognition of the systems engineering, architectural assessment, side of UCS, the focus has been on C2 policy and, to some extent, portfolio management.

4.4 OMB FEA. On February 6, 2002, the Office of Management & Budget (OMB) started requiring each government department and agency to produce their segment of the Federal Enterprise Architecture (OMB FEA). While this construct provides a single architecture standard for the federal enterprise, it has, so far, done little to bring the interoperability and ubiquitous information flow that is needed. "Right now, agencies' use of enterprise architecture is at a crossroads," said Randy Hite, Director, IT Architecture & Systems for the U.S. GAO [GCN, 2004]. "A great deal of effort has been put into developing an assortment of artifacts or components, but the real success of this whole EA discipline will hinge on whether or not these artifacts are actually used to effect change."

Ultimately the GAO's December 2003 Enterprise Architecture Maturity Management Framework (EAMMF) Report showed only two-tenths of one percent increase in the progress federal agencies made on EA initiatives in the last two years. In a nutshell, what GAO found when it measured the average maturity of agencies in adopting EA, was that, in 2001, the average level of maturity agency-wide was 1.74 on the GAO Maturity Scale of 1 to 5. And in 2003, the average was only 1.76.

GAO cited the two biggest challenges to the adoption of EA include a limited understanding of EA at the executive level, and a shortage of staff to adequately implement EA technologies. Since 2001, GAO reports, a growing number of agencies have identified these two issues as significant challenges to overcome. "Until these long-standing challenges are effectively

© Copyright 2007, Curts & Campbell

addressed, agencies' maturity levels as a whole are likely to remain stagnant, limiting their ability to effectively invest in IT," Hite says [GAO, 2006].

4.5 CCEA/NCC. In the Fall of 2004, the Continuity Communications Enterprise Architecture (CCEA) effort was initiated to investigate some of the deficiencies noted during 9/11, contingency planning exercises and other recent events.

The Continuity Communications Working Group (CCWG) was established as an interagency body reporting to the National Communications System (NCS) Committee of Principals (COP). The purpose of the CCWG was to oversee the development of a Continuity Communications Enterprise Architecture (CCEA) to support the performance of Federal Executive Branch (FEB) minimum essential functions under all circumstances, including crisis or emergency, attack, recovery, and reconstitution. The working group leveraged the existing Office of Management and Budget (OMB) Federal Enterprise Architecture (FEA) and related architectural frameworks to accelerate the establishment of an integrated, secure, standards-based, survivable, scalable, reliable, and converged EA supporting the FEB [ToR, 2004].

This effort grew out of the 2003 establishment of the Enduring Constitutional Government Coordination Council (ECGCC), commissioned to address various government continuity policies, programs, priorities and operational issues. The Office of Science and Technology Policy (OSTP) was tasked with developing an overall government Information Technology (IT) policy and migration strategy. OSTP requested the establishment of a Continuity Communications Working Group (CCWG) through the NCS Committee of Principals (COP) [CCEA, 2005] [7].

The initial report of the CCEA was delivered on 31 August 2005. Although the document "… and the CC EA data it represents, are the first steps toward defining an enterprise environment in the context of the Office of Management and Budget (OMB) Federal Enterprise Architecture (FEA) reference model …" it contained very little core architecture data and was a far cry from complete [CCEA, 2005].

While the CCEA effort continues at NCS a larger scale follow-on effort is being conducted, at least initially, out of another office within the Department of Homeland Security (DHS). The National Command Capability (NCC) is intended to be a superset of the CCEA in that it will develop and enterprise architecture for the FEB, State, local, tribal and first responders for all situations from normal, day-to-day operations through catastrophic events of all sorts. The first round of NCC discussions was held in late 2005 and early 2006.

4.6 DNI CIO. More recently, at the office of the Director of National Intelligence (DNI), the Chief Information Officer (DNI/CIO) has begun to publish the Enterprise Architecture (EA) for the Intelligence Community (IC). Like most of it's predecessors, however, we have yet another set of MS Word® documents, pdf files, PowerPoint® slides and other "pretty pictures" that may represent a moment in time but do little to further the goal of developing an investment strategy

[7] OSTP sponsored the Continuity Communications Enterprise Architecture (CCEA) in the 2004 – 2005 timeframe which later provided the foundation for the National Command Capability (NCC) architecture study in 2006. One of the authors, Dr. Curts, was the Deputy Program Manager for the original CCEA.

© Copyright 2007, Curts & Campbell

for portfolio management to produce a truly joint, fully connected, interoperable enterprise that will ensure that the right information gets to the right people at the right time. While some automated tools were beginning to be populated, this effort was significantly delayed in the Fall of 2006 due to a large turnover of support personnel.

4.7 And Others. In 1995 the ASD(C3I) formed the C4I Integration Support Activity (CISA) to develop a unified approach for development and evaluation of information architectures. One of CISA's working groups was the C4ISR Architecture Working Group (AWG) and AWG's final report concluded that there were a number (a very large number) of architectures out there. Each was well defined, though at a variety of levels, packed with useful information, and very beneficial to those who devised them. Most have a node somewhere on the periphery that is labeled "… connect to the … Army, Navy, Air Force, NSA, DIA, …" Unfortunately, as previously mentioned, these are typically the least well defined nodes in the architecture. Some are not defined at all. In truth, they might all be labeled, "A Miracle Happens Here!" Unfortunately, miracles are rare.

Several other good architectural and interoperability efforts have been initiated and most produced products that were/are useful to the agencies that conceived them. Here are a few:

- DII COE – Primarily hardware and software standards.
- JTA – Joint Warfighter Architecture. Provides "building codes."
- Copernicus – Naval Warfighter Architecture. Recognized the need for interoperability.
- DoN ITI and ITSG – provides DoN IT Architecture/Standards Guidance.
- INCA – Intelligence Community Architecture.
- Horizon – Air Force C4I for the Warfighter Architecture.

Obviously there are many architecture or architecture-related initiatives underway. But so far, the authors, the General Accounting Office (GAO) and others, in research independent from each other, are finding that no single product (nor consolidated set of interconnected products) has been produced which is useful from the "Big Picture" perspective of a totally integrated, interoperable, force much less the FEB.

Existing directives, and there are many, are very broad, general and uncoordinated within DoD, let alone between and amongst the services and agencies that make up DoD and the rest of the federal government. An even more diverse situation exists within the Intelligence Community (IC). Ongoing efforts to consolidate and simplify these controlling documents may soon remedy the situation. Still, while there is a great deal of support for interoperability concepts and much cooperation among agencies, there is currently little or no coordination in the detailed development of architectures and hence minimal progress.

Each agency develops architectures for their own purposes, at varying levels of detail, in their own formats, using the tools that happen to be available to them; few of which are interoperable. In general, the architectures developed by one agency are not readily comparable to those of another service or agency. Without the expenditure of a good deal of man-hours pouring through a large quantity of diagrams, tables and textual information, there is no good method of ensuring interoperability. There are few, if any, common terms of reference. Even the terms

© Copyright 2007, Curts & Campbell

"requirement" and "capability" are used differently amongst agencies. Terms, concepts and processes are not well defined, causing a great deal of miscommunication between agencies.

For some time now, DoD has allowed massively parallel efforts to continue, presumably in hopes that one would produce the perfect architectural construct. We have not yet been successful. Perhaps it is time to settle for a less perfect solution. General George Patton is said to have made the statement, "A good plan executed violently today is better than a perfect plan executed tomorrow." Similarly, Voltaire once wrote, "Best is the enemy of good."

5.0 WHERE DO WE GO FROM HERE?

If we consider Information Operations in the context of the larger, cradle-to-grave, womb-to-tomb, "big picture," we can better understand where we have been, where we would like to go, and how to get there.

Figure 3 was borrowed from a recent book on Architectures, Interoperability and Information Assurance [Curts, 2002]. From our perspective, there are two very weak links in this chain:

- Organizational constructs to support the process and
- Automated Tools as enablers.

Organizational considerations are, by far, the weakest link. Although we don't actually have the tools we need in widespread use, at least we know what they are (or should be) and some have already been adapted to architecture development.

© Copyright 2007, Curts & Campbell

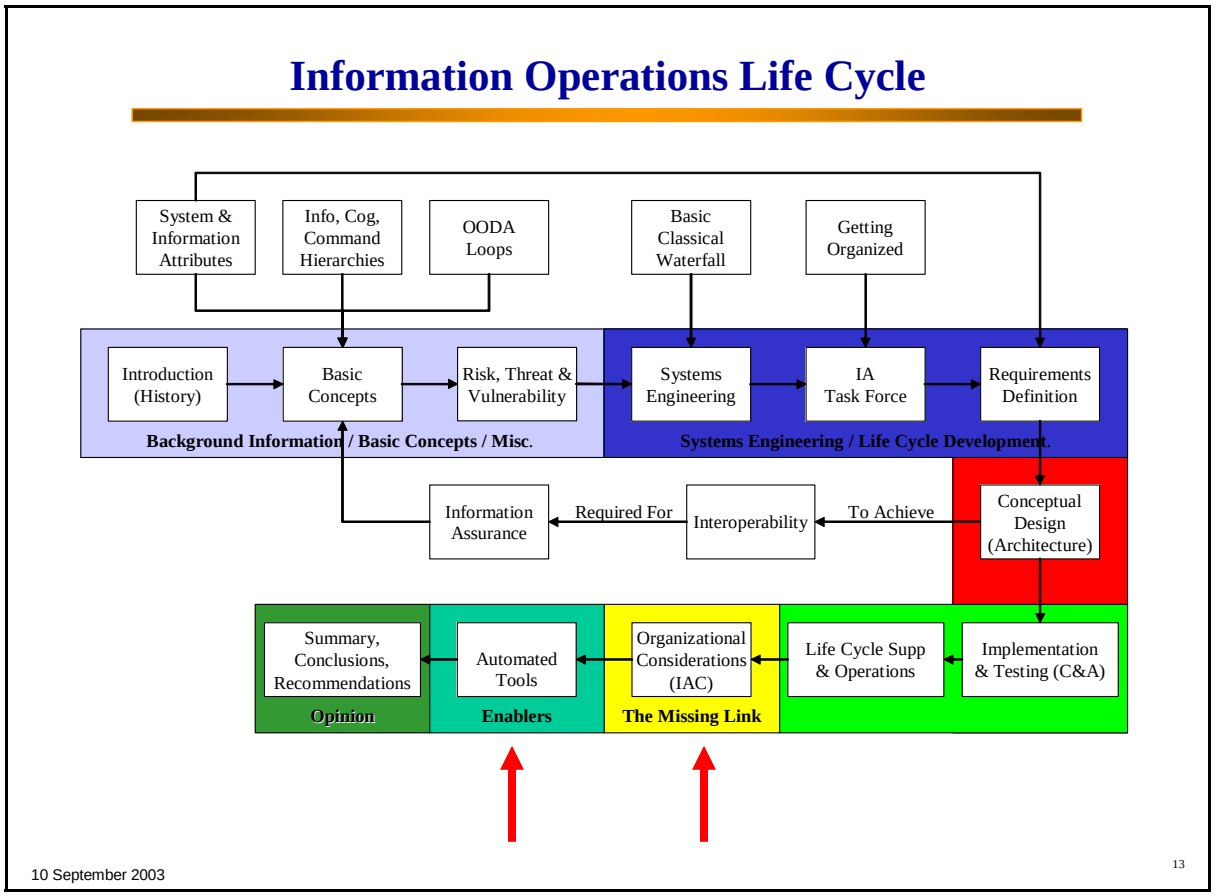

Figure 3: Information Operations Life Cycle

5.1 Given all of this, what is it that we need to do? As directed by the Deputy Secretary of Defense (DepSecDef), C2 will be managed as an integrated portfolio [Wolfowitz, 2004]. With respect to that C2 Portfolio, the intent is to define a series of mission threads and identify current Programs of Record (PoRs) that provide services and applications in support of those threads. From this existing portfolio we can define standards, and identify gaps, shortfalls, duplications and overlaps between the services and functional capabilities provided across PoRs, resulting in a clearer understanding of current enterprise capabilities available within the portfolio.

Simply stated, desired functional capabilities must be coordinated and integrated into a framework where C2 is viewed as a single unified enterprise. We do this by determining the efficiency and effectiveness of the C2 Portfolio using a repeatable, objective, defendable systems engineering process so that we can support informed, efficient and cost-effective budgeting and acquisition decisions (Figure 4).

© Copyright 2007, Curts & Campbell

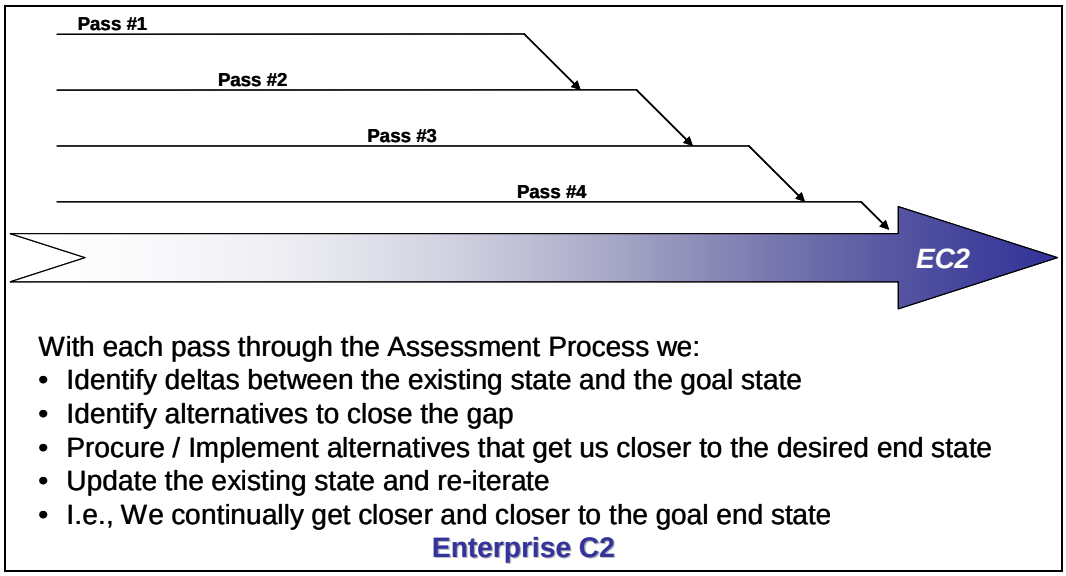

Figure 4: Migration toward Enterprise C2

As depicted in Figure 5, C2 Portfolio management is a long-term, iterative process of continual, sustained, refined evaluations, assessments, updates and modernization. Space limitations preclude a lengthy discussion of this graphic. The interested reader can find a more detailed discussion in [Curts, 2005]. Briefly the steps include:

a. *Define the Vision / Strategy / Policy / Goal – Not, strictly speaking, part of the systems engineering architecture process but a necessary starting point that initiates and supports a more detailed description of the goal.*
b. Develop a detailed *functional description* of the Goal processes and capabilities (the Desired End State).
c. Compile a list of existing programs / systems / services / processes / interfaces that make up the current infrastructure (the existing, baseline C2 Portfolio).
d. Develop a detailed *functional description* of the enterprise-wide capabilities provided by the interconnected programs / systems / services / processes / interfaces that make up the existing C2 Portfolio.
e. Assess the current C2 Portfolio against the processes and functional capabilities desired in the Goal or Desired End State.
f. Capture the results of the assessment process in the form of inter-related data sets in order to generate the required artifacts (using automated tools wherever possible).

© Copyright 2007, Curts & Campbell

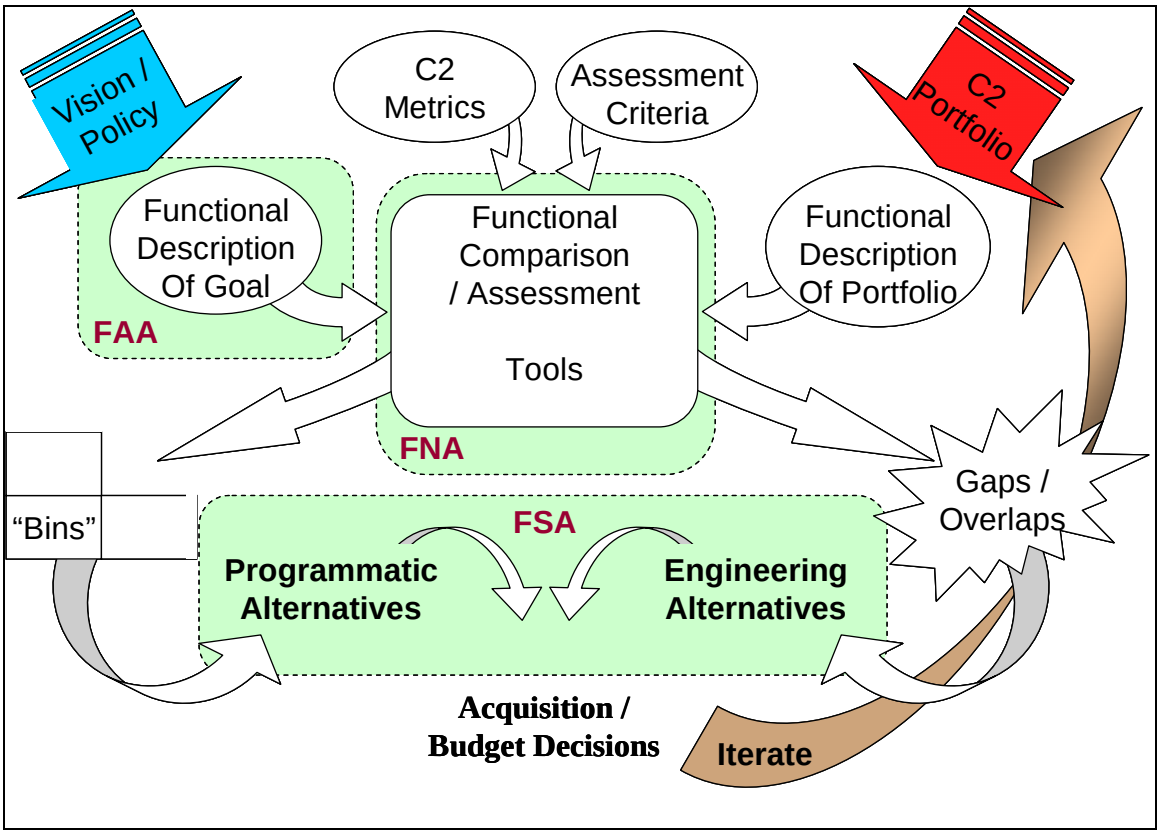

Figure 5: C2 Portfolio Management Process

g. Capture the results of the assessment process in the form of inter-related data sets in order to generate the required artifacts (using automated tools wherever possible).
h. Identify / define / prioritize programmatic and/or engineering alternatives to address the deficiencies noted during the assessment process above.
i. Application of Results / Programmatic Funding Decisions – Not, strictly speaking, part of the systems engineering architecture process itself, but the ultimate goal that the process is designed to support - Budgetary Decisions, Acquisition Decisions, Engineering Decisions
j. Ultimately, results end up in an updated C2 Portfolio at some future date whereupon the process begins anew.

6.0 SUMMARY / CONCLUSIONS

Architecture development (data collection, assessment, option development, design, testing and acquisition) is ***NOT*** a short term effort but rather a long-term and repetitive process. To date, no large scale, automated architecture assessment process has managed to stay alive through more than one or two iterations. For the most part, DoD has not captured the underlying data necessary for a truly repeatable, defendable, robust assessment. However, if we take the time to investigate the significant impact that some small, relatively short-lived initiatives have had in the past, it becomes obvious that the concepts, processes and methodologies associated with a

© Copyright 2007, Curts & Campbell

well defined, repeatable, enterprise-wide, systems engineering, architecture development process have merit and would significantly increase the effectiveness and efficiency of C2.

If we are ever to achieve our goal, the concept of a single unifying construct and a repeatable, defendable process for portfolio management (Figure 5), must receive support at the highest levels of DoD. This plan provides a start and is offered as a first step toward a DoD-wide, interoperable, Enterprise Architecture.

7.0 RECOMMENDATIONS

We could discuss the issues for years (and have). Perhaps it would be more useful to choose a set of actions that we might actually be able to accomplish in a reasonable timeframe and press forward. After a decade or more of study, the authors have identified 6 recommendations for getting a better handle on the problem. The following are a set of relatively simple things that might allow us to make some significant progress.

First, as twice reiterated by the DSB, some high-level guidance and control must be established for the entire enterprise.

> *"The Defense Science Board and other major studies have concluded that one of the key means for ensuring interoperable and cost effective military systems is to establish comprehensive architectural guidance for all of DoD." [USD(A&T), 1997]*

Next, we must settle upon a common lexicon. If architectures are ever to be interoperable, the developers of those documents must be able to communicate efficiently and effectively. Terms such as architecture, master plan, requirement, capability, etc. must be defined and used consistently by all players.

Third, a standardized, a well-defined, automated architectural process would significantly simplify the evolution of architectures while adding a certain amount of rigor, reproducibility, and confidence to the procedure. Earlier works, [Curts, 1989a], [Curts, 1989b], [Curts, 1990] and [Curts, 1995] have discussed these concepts in greater detail. The process must, as a minimum, contain well defined: authority, designated cognizant activities, processes, milestones, architectural outlines and formats, deliverables, documentation, and maintenance/update schedules.

Fourth, we must define and adopt architecture development, definition, maintenance and interface standards as necessary:

- to ensure: interoperability and connectivity of architectures, consistency, compliance with applicable directives, and architectural information dissemination;
- to facilitate: implementation of policies and procedures, acquisition strategies, systems engineering, configuration management, and technical standards; and
- to standardize: terms of reference, modeling tools, architecture data elements, architecture data structures, hardware and software interfaces, architectural representations and architectural scope, and level of detail/abstraction.

© Copyright 2007, Curts & Campbell

The goal should not be forced procurement of a single, standard system that performs some specific set of functions. The real issue, at least in the near term, is not "Who is using what system?", but rather "Are these various systems compatible/interoperable?" In other words, all that we really need, at least to start, are interface/interoperability standards. It is time to stop investigating architectural concepts and start defining/building joint, interoperable, standardized architectures.

Fifth, any architecture effort must produce meaningful interim results if it is to survive. Decision makers can not wait 5, 10, 20 years for answers. Moreover, we can not afford to fund such long term, expensive projects without solid, incremental Return On our Investment (ROI). Architectures can and should produce meaningful, albeit limited, results in months rather than years.

Finally, the most important single concept is automation. The vast quantities of data required to compile and manipulate an architecture within the ever changing operational and fiscal environments simply can not be completed manually in time to have any significant impact. If we successfully capture the underlying data, DoDAF, OMB FEA and other artifacts can be generated on the fly. More importantly, we can employ automated tools to analyze the data from any desired perspective. A more detailed discussion of automated architecture tools can be found in [Curts, 1990] and [Curts, 2003].

8.0 A FINAL WORD: THE NEXT MAJOR HURDLE

A major technical goal of the next ten years will be the utilization of an architecture that allows interoperability between C4I systems and Modeling & Simulation (M&S). Current technologies do not support such interoperability, without unique hardware (human-in-the-loop in many cases) and software. The goal within the next decade should be to allow the majority of military C4I systems to "plug-and-play" to the majority of military M&S applications and exchange information without having to build unique interfaces. In other words, to give end-users the needed interoperability and reusability of M&S programs running in a common environment. This will provide an increased ease-of-use for the warfighter community. And this will promote the ability to train warfighters on the same C4I systems that they will use in the field, at reduced training and development costs for specialized interfaces to models. Again, the Defense Science Board Task Force on Readiness:

> *"Modeling and simulation technology should be exploited to enhance joint and combined training and doctrine. It offers a tremendous opportunity to leverage our existing training at all levels through enhancement or even replacement where appropriate after thorough review." [DSBR, 1994]*

© Copyright 2007, Curts & Campbell

Acronyms

A Spec	A Specification (A system development specification)
ACC	Architecture Coordination Council (DoD)
ADPA	American Defense Preparedness Association (currently NDIA)
APCO	Association of Public Safety Communications Officers International
ASD(C3I)	Assistant Secretary of Defense, Command, Control, Communications and Intelligence – renamed ASD(NII)
ASD(NII)	Assistant Secretary of Defense, Networks and Information Integration – formerly ASD(C3I)
AWG	Architecture Working Group
BDA	Battle Damage Assessment
C&A	Certification and Accreditation
C2	Command and Control
C4	Command, Control, Communications, and Computers
C4I	Command, Control, Communications, Computers, and Intelligence
C4ISP	C4I Support Plan
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
C4ISR AWG	C4ISR Architecture Working Group (one of CISA's working groups)
CADM	C^4ISR Core Architecture Data Model
CALCM	Conventional Air Launched Cruise Missile
CAOC	Combined Air Operation Center
CASE	Computer Aided Systems Engineering
CCA	Clinger-Cohen Act – aka Information Technology Management Reform Act of 1996
CCEA	Continuity Communications Enterprise Architecture
CCWG	Continuity Communications Working Group
CENTCOM	U. S. Central Command
CIO	Chief Information Officer
CIP	Common Intelligence Picture
CISA	C4I Integration Support Activity
CJCSI	Chief, Joint Chiefs of Staff Instruction
CNO	Chief of Naval Operations
COE	Common Operating Environment
COP	Committee of Principals
COP	Common Operating / Operational Picture
CTAPS	Contingency Tactical Air Planning System
DDDS	Defense Data Dictionary System
DepSecDef	Deputy Secretary of Defense
DHS	Department of Homeland Security
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DNI	Director of National Intelligence
DoD	Department of Defense
DoDAF	Department of Defense Architecture Framework
DoN	Department of the Navy
DSB	Defense Science Board
EA	Enterprise Architecture
EAMMF	Enterprise Architecture Maturity Management Framework
ECG	Enduring Constitutional Government
ÉCGCC	Enduring Constitutional Government Coordination Council
EOP	Executive Office of the President
FAA	Functional Area Analysis (JCIDS)
FAFIM	Functional Architecture Framework for Information Management
FEA	Federal Enterprise Architecture
FEB	Federal Executive Branch
FNA	Functional Needs Analysis (JCIDS)

© Copyright 2007, Curts & Campbell

FSA	Functional Solutions Analysis (JCIDS)
FTP	File Transfer Protocol
FY	Fiscal Year
GAO	Government Accountability Office – formerly General Accounting Office
GiG	Global Information Grid
GPRA	Government Performance and Results Act of 1993
IA	Information Assurance
IAC	Information Assurance Center
IC	Intelligence Community
IEEE	Institute of Electrical and Electronics Engineers
INCA	Intelligence Community Architecture
IT	Information Technology
ITI	Information Technology Infrastructure (DoN)
ITMRA	Information Technology Management Reform Act – aka Clinger-Cohen Act of 1996
ITSG	Information Technology Standards Guidance
JCIDS	Joint Capabilities Integration and Development System
JCS	Joint Chiefs of Staff
JICCENT	Joint Intelligence Center – Central Command
JINTACCS	Joint Interoperability of Tactical Command & Control Systems
JITC	Joint Interoperability Test Command
JITF	Joint Interface Test Force
JTA	Joint Technical Architecture
M&S	Modeling and Simulation
MAPE	Monitor, Analyze, Plan, and Execute
MEF	Mission Essential Functions
MISREP	Mission Report
MTF	Message Text Format
NAS	National Airspace System (Federal Aviation Administration)
NATO	North Atlantic Treaty Organization
NCC	National Command Capability
NCOW	Net-Centric Operations and Warfare
NCS	National Communications System
NCW	Network Centric Warfare
NDIA	National Defense Industrial Association (formerly NSIA/ADPA)
NSIA	National Security Industrial Association (currently NDIA)
NWTDB	Naval Warfare Tactical Data Base
OASD	Office of the Assistant Secretary of Defense
OIF	Operations Iraqi Freedom
OMB	Office of Management and Budget
OODA	Observe, Orient, Decide, Act
OSTP	Office of Science and Technology Policy
OV	Operational Views (DoDAF artifacts)
PM	Portfolio Management
PODM	Plan, Organize, Direct, Monitor
POM	Program Objective Memorandum
PoR	Program of Record
ROI	Return on Investment
SBA	Standards Based Architecture
SE	Systems Engineering
SHADE	Shared Data Environment
SPAWAR	Space and Naval Warfare Systems Command
SSC-C	SPAWAR Systems Center – Charleston
SV	System Views (DoDAF artifacts)
TAFIM	Technical Architecture Framework for Information Management
TBMCS	Theater Battle Manager Core Systems
TLAM	Tactical Land Attack (Cruise) Missile

© Copyright 2007, Curts & Campbell

TTP	Tactics, Techniques and Procedures
UCS	Unified Command Structure
USAF	United States Air Force
USD	U. S. Under Secretary of Defense
USD(A&T)	Under Secretary of Defense, Acquisition and Technology – renamed USD(AT&L)
USD(AT&L)	Under Secretary of Defense, Acquisition, Technology and Logistics – formerly USD(A&T)
USN	United States Navy
WSA&E	Warfare Systems Architecture and Engineering
WSV	Weapon System Video

© Copyright 2007, Curts & Campbell

References

[Anno, 1988] Anno, Stephen and William E. Einspahr, "The Grenada Invasion," in Command and Control Lessons Learned: Iranian Rescue, Falklands Conflict, Grenada Invasion, Libya Raid. Maxwell Air Force Base, AL: Air University Press, Air War College Research Report, No. AU-AWC-88-043, 1988. Reprinted as an extract from the original report by the U.S. Naval War College Operations Department, NWC 2082, 40, 42 [On-line]. URL: http://www.fas.org/man/dod-101/ops/urgent_fury.htm.

[Bjorklund, 1995] Bjorklund, Raymond C. The Dollars and Sense of Command and Control. Washington, DC: National Defense University Press, 1995, pp. 73-75.

[Boyd, 1986] Boyd, John. Patterns Of Conflict, December 1986. Unpublished study, 196 pages.

[Bradley, 2004] Bradley, Carl M. "Intelligence, Surveillance And Reconnaissance In Support Of Operation Iraqi Freedom: Challenges For Rapid Maneuvers And Joint C4ISR Integration And Interoperability." Published by the Joint Military Operations Department, Naval War College, 686 Cushing Road, Newport, RI 02841-1207; September 2, 2004.

[CADM, 1997] C4ISR Core Architecture Data Model, Version 1.0, 15 September 1997.

[CAF, 1997] C4ISR Architecture Framework, Version 2.0. Washington, DC: C4ISR Architecture Working Group (AWG), 18 December 1997.

[CCEA, 2005] United States Federal Executive Branch Continuity Communications Enterprise Architecture (Initial Report). Arlington, VA: Continuity Communications Working Group (CCWG), 31 August 2005.

[Cebrowski, 1998] Cebrowski, USN, Vadm Arthur K. "Network-Centric Warfare – Its Origin and Future." U.S. Naval Institute Proceedings, p. 31, January, 1998.

[Charles, 2004] "Capabilities Based Acquisition … From Theory to Reality." Chips Magazine, 38-39, Summer 2004. Charleston, SC: Space & Naval Warfare Systems Center, Charleston, 2004.

[CIMPIM, 1993] Corporate Information Management Process Improvement Methodology for DOD Functional Managers, Second Edition. Arlington, VA: D. Appleton Company, 1993, p. 152.

[CISA, 1996] C4ISR ITF Integrated Architectures Panel, C4ISR Architecture Framework Version 1.0. CISA-0000-104-96 dated 7 June 1996.

[CJCS6212, 1995] CJCS Instruction 6212.01A, Compatibility, Interoperability, and Integration of Command, Control, Communications, Computers, and Intelligence Systems. Washington, DC: Joint Chiefs of Staff, 30 June 1995.

[Clements, 1996] Clements, Paul C. and Linda M. Northrop. Software Architecture: An Executive Overview (CMU/SEI-96-TR-003). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1996.

[Clemins, 1998] Clemins USN, ADM Archie. "Remarks to AFCEA Asia Pacific TECHNET '98." Honolulu, HI: Asia Pacific TECHNET Conference, 5 Nov 1998.

© Copyright 2007, Curts & Campbell

[CSC, 1995] DoD Architecture Review, 2 Volumes. Falls Church, VA: Computer Sciences Corporation, 1995. Vol. 1, p. 3.

[Curts, 1989a] Curts, Raymond J. "A Systems Engineering Approach to Battle Force Architecture." Unpublished research. Fairfax, VA: 1989.

[Curts, 1989b] Curts, Raymond J. "An Expert System for the Assessment of Naval Force Architecture." Unpublished research. Fairfax, VA, 1989.

[Curts, 1990] Curts, Raymond J. "Automating the Architecture Process." Briefing/Lecture. Washington, DC: Space and Naval Warfare Systems Command, 1990.

[Curts, 1995] Curts, Raymond J. "Inference Methodologies in Decision Support Systems: A Case Study." Information and Systems Engineering. Amsterdam, The Netherlands: IOS Press, 1995.

[Curts, 2002] Curts, Raymond J. and Douglas E. Campbell. Building a Global Information Assurance Program. New York, NY: Auerbach Publications, 2002.

[Curts, 2003] Curts, Raymond J. and Douglas E. Campbell. "Analyzing C4isr Architectures Through An Automated Data Visualization Environment." Proceedings 2003 CCRTS. Washington, DC: Command & Control Research Program (CCRP), 2003.

[Curts, 2005] Curts, Raymond J. "Enterprise C2 (EC2) Systems Engineering (SE) Overview." Arlington, VA: CommIT Enterprises, Inc., 2005.

[Curts, 2006] Curts, Raymond J. and Douglas E. Campbell. "Rethinking Command & Control." Proceedings 2006 CCRTS. San Diego, CA: Command & Control Research Program (CCRP), 2002.

[Dickerson, 2003] Dickerson, C. E., S. M. Soules, M. R. Sabins and S. H. Charles. Using Architectures for Research, Development and Acquisition. Reston, VA: BAE Systems, 2003.

[DISA, 2003] Defense Information Systems Agency. "What is the Joint Global Command & Control Systems." http://gccs.disa.mil/gccs/, last updated May 19, 2003.

[DoD4630, 1998] DoD Directive 4630.5, "Compatibility, Interoperability, and Integration of Command, Control, Communications and Intelligence (C^3I) Systems." Washington, DC: Department of Defense (DoD), 1998.

[DoD8020, 1993] DoD 8020.1-M, Functional Process Improvement (Draft). Washington, DC: Department of Defense (DoD), 1993.

[DoD8320, 1994] DoD 8320.1-M, DoD Data Administration Procedures. Washington, DC: Department of Defense (DoD), March, 1994.

[DoD8320, 1998] DoD 8320.1-M-1, Draft DoD Data Element Standardization Procedures. Washington, DC: Department of Defense (DoD), February, 1998.

[DoDAF, 2003] DoD Architecture Framework, Version 1.0. Washington, DC: DoD Architecture Framework Working Group (AFWG), 31 August 2003.

[DoDAF, 2004] DoD Architecture Framework, Version 1.0, Deskbook. Washington, DC: DoDAF Working Group (AFWG), 9 February 2004.

© Copyright 2007, Curts & Campbell

[DoDD4630.5, 1992] DoD Directive 4630.5, Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C^3I) Systems. Washington, DC: Department of Defense (DoD), 12 November 1992.

[DoDD4630.8, 1992] DoD Directive 4630.8, Procedures for Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C^3I) Systems. Washington, DC: Department of Defense (DoD), 18 November 1992.

[DSBGS, 1993] Defense Science Board (DSB). Report of the Defense Science Board Task Force on Global Surveillance. Washington, DC: Office of the Under Secretary of Defense for Acquisition and Technology (USD(A&T)), December 1993.

[DSBR, 1994] Defense Science Board (DSB). Report of the Defense Science Board Task Force on Readiness. Washington, DC: Office of the Under Secretary of Defense for Acquisition and Technology (USD(A&T)), June 1994.

[Endicott, 1995] Endicott, George. Official Electronic Mail Communication to Dr. Curts. Arlington, VA: Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C^3I)), 11 April 1995.

[Erickson, 1998] Erickson, CDR James, et al. "Impact of Joint Technical Architecture on Navy Acquisition." Program Manager (PM), 34-38, Nov-Dec, 1998.

[FEACRM, 2006] Federal Enterprise Architecture (FEA) Consolidated Reference Model (CRM) Document, Version 2.1. Washington, DC: Office of Management and Budget (OMB), December 2006.

[GAO, 1998] Joint Military Operations: Weaknesses in DOD's Process for Certifying C^4I Systems' Interoperability. GAO/NSIAD-98-73. Letter Report dated 03/13/98.

[GAO, 2006] Hite, Randolph C., Director, Information Technology Architecture And System Issue, United States Government Accountability Office (GAO) on GAO Report Number GAO-06-831, Enterprise Architecture: Leadership Remains Key to Establishing and Leveraging Architectures for Organizational Transformation. Released September 12, 2006.

[GCN, 2004] "The State of EA: GOA Report." Government Computer News, 2004.

[Giambastiani, 2003] Statement of Admiral E. P. Giambastiani, Commander, U.S. Joint Forces Command, Before the House Armed Services Committee, October 2, 2003.

[GRCI, 1998] Information Warfare White Paper for Space and Naval Warfare Systems Command (SPAWAR). Information Warfare Program Directorate (PD-16). Vienna, VA: GRC International, March 1998.

[IEEE, 1984] Jay, Frank, ed. IEEE Standard Dictionary of Electrical and Electronics Terms. New York, NY: IEEE, 1984, p. 915.

[ITSG, 1998] Information Technology Standards Guidance – Information Management. Final Draft Version 1.0. Washington, DC: Department of the Navy, 1998.

[JITC, 1998] C^4I Interoperability–JITC Certification Process. JITC Home Page, 21 Oct 1998.

[JTA, 1996] Department of Defense Joint Technical Architecture, Version 1.0, 22 August 1996.

[JTA, 2003] Department of Defense Joint Technical Architecture, Version 6.0, 3 October 2003.

© Copyright 2007, Curts & Campbell

[Kerr, 2005] Jennifer C. Kerr. "Lack of Interoperability Hampered Hurricane Responders." Associated Press. 16 October 2005

[Mathwick, 1997] Mathwick, James E. "Database Integration, Practical Lessons-Learned." San Diego, CA: DoD Database Colloquium, 1997.

[McKay, 2006] Jim McKay. "The Technology Trap." Emergency Management Magazine. November 2006.

[Michaels, 1999] "DoN Data Interoperability." Briefing to Mr. Dan Porter, DoN CIO. Arlington, VA: GRC International, 18 February 1999.

[NATO, 1999] U.S. Mission to NATO, "Joint Statement to Senate Armed Services Hearing on Kosovo: Lessons Learned," The U.S. Mission to NATO Security Issues Digest, 203 (Oct. 21, 1999)

[NDIA, 1999] Information Assurance Study. Fairfax, VA: C4ISR Committee of the National Defense Industrial Association (NDIA), July 1999.

[NSIA, 1997] "The Contingency Tactical Air Planning Systems (CTAPS)." Command and Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) Interoperability and Integration Study. Washington, DC: National Security Industrial Association (NSIA), 1997.

[OMB FEA, 2004] Guidelines for Enterprise Architecture Assessment Framework, v2. Washington, DC: Office of Management & Budget, 2004.

[Paige, 1993] Paige, Emmett. Selection of Migration Systems. ASD (C3I) Memorandum. Washington, DC: Department of Defense, 12 November 1993.

[Pike, 2000] Pike, John. "Tasking, Processing, Exploitation & Dissemination (TPED), TPED Analysis Process (TAP)." Federation of American Scientists (FAS), Intelligence Resource Program, January 29, 2007. Available at: http://www.fas.org/irp/program/core/tped.htm.

[Robinson, 2004] Robinson, Col Brian. Global Information Grid (GIG) Systems Engineering (SE) Oversight and the Role of the TCO. Washington, DC: Office of the Assistant Secretary of Defense (Networks and Information Integration) (OASD(NII)), 17 Feb 2004.

[Snyder, 1993] Snyder, Frank M. Command and Control: The Literature and Commentaries. Washington, DC: National Defense University Press, 1993, 111.

[TAFIM, 1994] U.S. Department Of Defense. Technical Architecture Framework For Information Management (TAFIM), Volumes 1-8, Version 2.0. Reston, VA: DISA Center for Architecture, 1994.

[Temin, 1996] Temin, Thomas, ed. "Mishmash at Work (DoD Systems in Bosnia are not Interoperable)." Government Computer News 15, 7 (April 1996): 28.

[ToR, 2004] Draft Terms of Reference For The Continuity Communications Working Group, August 2004.

[USD(A&T), 1996] "Implementation of the DoD Joint Technical Architecture." USD(A&T) and ASD(C^3I) Joint Memorandum. Washington, DC: Office of the Under Secretary of Defense for Acquisition and Technology and the Assistant Secretary of Defense for Command, Control, Communications and Intelligence, 1996.

© Copyright 2007, Curts & Campbell

[USD(A&T), 1997] USD (A&T), ASD (C3I), JS/J6 Memorandum, Subject: DoD Architecture Coordination Council (ACC), 14 January 1997.

[Webster, 1984] Webster's II: New Riverside University Dictionary. Boston, MA: The Riverside Publishing Company, 1984.

[Wolfowitz, 2004] Wolfowitz, Paul. Memorandum: Information Technology Portfolio Management. Deputy Secretary of Defense, 22 March 2004.

[WSA&E, 1988] "Warfare Systems Architecture & Engineering." Briefing to ADM Chang. Washington, DC: Space and Naval Warfare Systems Command, 1988.

© Copyright 2007, Curts & Campbell

Vita

Raymond J. Curts, PhD, CDR, USN, (Ret.) was born December 2, 1946 in Philadelphia, Pennsylvania and is an American citizen. He graduated from Vandalia Community High School, Vandalia, Illinois in 1965. He earned his Bachelor of Science in Aeronautical and Astronautical Engineering from the University of Illinois in 1970 and was commissioned an Ensign in the United States Navy. In December 1972 he earned his wings as a Naval Aviator and was assigned to the U.S. Naval Base at Guantanamo Bay, Cuba. Returning to the continental United States in 1976, he served as an instructor pilot in the Navy's Advanced Jet Training Command in Beeville, Texas where he earned a Master's degree in Management and Business Administration from Webster University of St. Louis, Missouri. During tours of duty in Norfolk, Virginia; Rota, Spain; and Key West, Florida, he served as the A-3B NATOPS Model Manager (NMM), the Training Model Manager (TMM) and the A-3B Director of Training, and was responsible for all A-3B aircrew and maintenance training Navy-wide. CDR Curts' final tour was at the Space and Naval Warfare Systems Command Headquarters (SPAWAR) in Washington, DC where he spent five years as the Navy's Electronic Warfare Architect. During this time he earned a Ph.D. in Information Technology from George Mason University and retired from active duty in 1992. Since that time Dr. Curts has worked in support of numerous DoS and DoD programs as a defense contractor and has conducted a variety of studies in the areas of Information Architectures, Interoperability and Information Assurance. He was a primary contributor to the Navy's Information Warfare Master Plan and Acquisition Strategy and was responsible for a complete re-write of the U.S. State Department's Information Assurance Policies and Procedures. Later Dr. Curts supported the Director, C2 Policy at ASD(NII) interfacing to DoD C2 architecture efforts. Currently, Dr. Curts supports the Chief Information Officer in the Director of National Intelligence, serves as an Adjunct Professor of Information Technology and Engineering at both George Mason and George Washington Universities, and is involved in standards making and investigative bodies associated with IEEE, NDIA, CCRP, ITAA, NIAP, AFCEA, and AOC among others.

LCDR Douglas E. Campbell, Ph.D., (USNR-R, Ret.) was born on May 9, 1954 in Portsmouth, Virginia, and is an American citizen. He graduated from Kenitra American High School, Kenitra, Morocco, in 1972. He received his Bachelor of Science degree in Journalism from the University of Kansas in 1976 and was immediately commissioned as an Ensign in the United States Navy. He joined the U.S. Naval Reserve Program as an Intelligence Officer in 1980 and was transferred to the Retired Reserves as a Lieutenant Commander on 1 June 1999. Dr. Campbell received his Master of Science degree from the University of Southern California in Computer Systems Management in 1986 and his Doctor of Philosophy degree in Computer Security from Southwest University in New Orleans (Kenner), Louisiana, in 1990. Dr. Campbell is president and CEO of Syneca Research Group, Inc., a certified 8(a) and a certified Small & Disadvantaged Business entity under the U.S. Small Business Administration's program. Syneca is currently supporting DoD, DHS, FAA, VA and others in command & control, physical and computer security, system engineering and IT support services.

© Copyright 2007, Curts & Campbell