United States Air Force Scientific Advisory Board

Report on

Domain Integration

Executive Summary and Annotated Brief

SAB-TR-05-03
July 2005

DISTRIBUTION AUTHORIZED
In accordance with AFI 61-204 and DODD 5230.24, distribution statement A, this document is approved for public release; distribution is unlimited.

This report is a product of the United States Air Force Scientific Advisory Board Study Committee on *Domain Integration*. Statements, opinions, findings, recommendations, and conclusions contained in this report are those of the Study Committee and do not necessarily represent the official position of the United States Air Force or the United States Department of Defense.

United States Air Force Scientific Advisory Board

Report on

Domain Integration

Executive Summary and Annotated Brief

(This page intentionally left blank.)

Executive Summary

Introduction

The Domain Integration ad hoc study addresses the effective manipulation and transfer of information among warfighters by predominantly machine-to-machine means. More specifically, the vision derived from the Terms of Reference[1] is:

The ability to horizontally integrate multi-intelligence (multi-INT) information from space, air, and ground at a machine-to-machine level will enable the Air Force to rapidly and accurately integrate data and information across domains to address time sensitive targets.

The study team reviewed current capabilities and technologies, identified an architectural approach, determined the needed technology advancements, and recommends a path through experimentation to fielding.

Background

Warfighters incur significant delays when humans must manually manipulate data to provide direct or cognitive integration of multiple sources of data. Moreover, information is lost or modified in the process such that the original meaning or value is damaged.

This study is the third in a series of (coupled) Air Force Scientific Advisory Board (AF SAB) studies. The 2003 AF SAB study "Technology for Machine-to-Machine Intelligence, Surveillance, and Reconnaissance Integration" postulated a construct in which different domains (e.g., signals intelligence (SIGINT), imagery intelligence (IMINT), and measure and signature intelligence (MASINT)), each with its own internal "domain architecture," became components of a common information architecture to enable information sharing without paying the cost of full pair-wise integration of the component systems. The 2004 AF SAB study "Networking to Enable Coalition Operations" (NECO) proposed a high-level information architecture for addressing combined air operations center (CAOC) needs at the operational level. The NECO study identified the need to revise the security culture to one of "need-to-share" vice "need-to-know," and to post a metadata tag with information that defined the content, context, and data structure such that rule-based and role-based releasability processes could be implemented.

The Domain Integration study was chartered to take the next step – develop a detailed definition of the architecture to enable rapid domain integration, conformant to the NECO requirements.

The Problem

Joint and coalition operations involve many diverse stakeholders with differing cultures and responsibilities. In addition, there is a high degree of heterogeneity and redundancy among organizations, processes, and systems. A critical problem in integrating systems that cross these

[1] See Appendix A

largely autonomous domains stems from inconsistent data/information models and associated databases. These inconsistencies lead to both syntactic and semantic confusion.

Across domains there is very little shared understanding of data/information that would enable significant machine-to-machine interactions. A key to achieving machine-to-machine automation is consistent metadata[2] for all information exposed for use across the net-centric environment.

Currently, there are limited metadata available from existing and emerging systems. Further, metadata schemas and descriptions often are inadequate and inconsistent. There is an existing policy, "Air Force Information and Data Strategy Policy" dated 3 March 2004, but progress in implementing that policy is not sufficient to achieve system of systems interoperation in the near-term.

Domains and Communities of Interest

Domains are affinity groups that have been more or less successful in producing a dataset of interest in support of a specific mission or missions. Historically, a domain was successful if the necessary Responsibility, Authority, Accountability, and Resources (RAAR) were assigned to achieve the mission, but RAAR (or the lack of it) also inherently determined the content, boundaries, and limitations of the domain. Since these domains were created at different times for different purposes by many different organizations, their definition, content, and format are almost always incompatible. Thus, integrating (or, more properly, making interoperable) these domains requires overcoming these legacy-driven incompatibilities in some way.

The execution of missions often requires capabilities, information and resources from multiple domains, which leads to the formation of Communities of Interest (COI). COI is the inclusive term used to describe collaborative groups of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes and who therefore must have shared vocabulary for the information that they exchange. The COI may be formed or aggregated across domain and organizational boundaries and may be expedient/fleeting in response to emerging needs, or may be long lived/institutional.

Architecture

Currently, the Air Force is organized such that interactions within a domain (stovepipe) are facilitated but interactions among domains are restricted and preclude machine-to-machine integration. Within the stovepipe, integration has produced monolithic systems that result in a lack of flexibility and responsiveness to demands outside of the stovepipe and a brittleness that is exposed when change is required. However, the monolithic systems provide efficient solutions to the problems for which they were designed.

The Service Oriented Architecture (SOA) concept and initial SOA architecture were originally developed to deal effectively with the large number of extremely heterogeneous domains resident on the Internet. Internet-based SOAs facilitate the creation of Web COIs to

[2]Metadata is "data about data." As such, they describe the context, content, and structure of the data so that data can be catalogued and accessed with efficiency and accuracy.

assemble and integrate data sources from multiple different domains in a manner consistent with the time, resource, and purpose-based needs of each COI.

DOD has adopted the SOA approach in its development of the Global Information Grid (GIG). Specifically, the DOD has identified nine specific services that the GIG will offer to subscribers, and the GIG program called Net-Centric Enterprise Services (NCES) is charged with the development and provision of these Services to GIG users.

Degree of Integration

Our study objective is "domain integration," which we have defined as the implementation of (widely) shared functional interfaces between domains which allow (but do not necessarily require) access to, use, or control of resources and capabilities within the domains. In this definition, "integration" refers to a satisfactory degree of interoperation. Domains are integrated if the separate capabilities can work together without any "seams" that pose obstacles to the warfighter.

Users should not care how their demands are satisfied. It is enough to make the right information available, machine-to-user *and* machine-to-machine. Very often, the best (fastest, cheapest, and most effective) way to achieve this is not to build an integrated monolith – instead, provide systems and information that can be quickly composed to satisfy changing needs. *Domain interoperation*, not (total) domain integration, is in general a more appropriate objective.

Achieving the Vision

The need for commonly accepted and widely used domain integration architecture has been recognized and advocated by the Air Force Scientific Advisory Board for some time. However, it is important to test the applicability of this proposed approach to the challenging domain integration problems the Air Force faces, especially at the tactical level.

In the initial direction, we were provided a specific problem, expressed in the form of a mission vignette. This vignette in an expanded form was adopted as the basis for assessing current shortfalls and defining the steps, with associated technologies, which would move the information in a machine-to-machine architecture. Our team did a "chair fly through" the scenario to document how the proposed architecture could address "domain integration" and includes elements of non-traditional intelligence, surveillance, and reconnaissance (ISR) as they might contribute.

Recommendations

Recommendation 1. Exploit GIG Enterprise Services (GIG-ES) to achieve interoperability

NCES is a new-start program intended to develop the core infrastructure services for the GIG. The success of this program is important to the Air Force – it needs to be built, and built right. It is similarly important that the Air Force experience gained should be transferred to the NCES program.

Recommendation 2. Conduct a limited technology experiment to explore the limits of the SOA

The most efficient and timely method of developing fieldable capability based on an SOA is via a sustained series of experiments, with the best ideas leading quickly to operational demonstration and use. As a first step toward fielding operational capability based on a SOA implementation, a limited technology experiment should be conducted in a laboratory testbed environment.

The testbed should be used to mature the SOA implementation for the mission thread to the point that it can be taken to the Distributed Mission Operations Center (DMOC) for operational testing in a realistic environment without unnecessarily impacting the DMOC training responsibilities.

Recommendation 3. Conduct operational experiments for virtual domain integration

An operational experiment is critical to validating the architecture and the technical concepts. Moreover, it provides the opportunity for operational personnel to experiment with the capabilities and provide valuable feedback to the technical team; and to devise concept of operations (CONOPS) and tactics, techniques, and procedures (TTPs) for the eventual fielding of the capability.

Elements of the Air Force distributed mission operations (DMO) infrastructure (hardware, software, networking, and personnel) appears to be ideal for operational experimentation in addition to its primary role of training and operations.

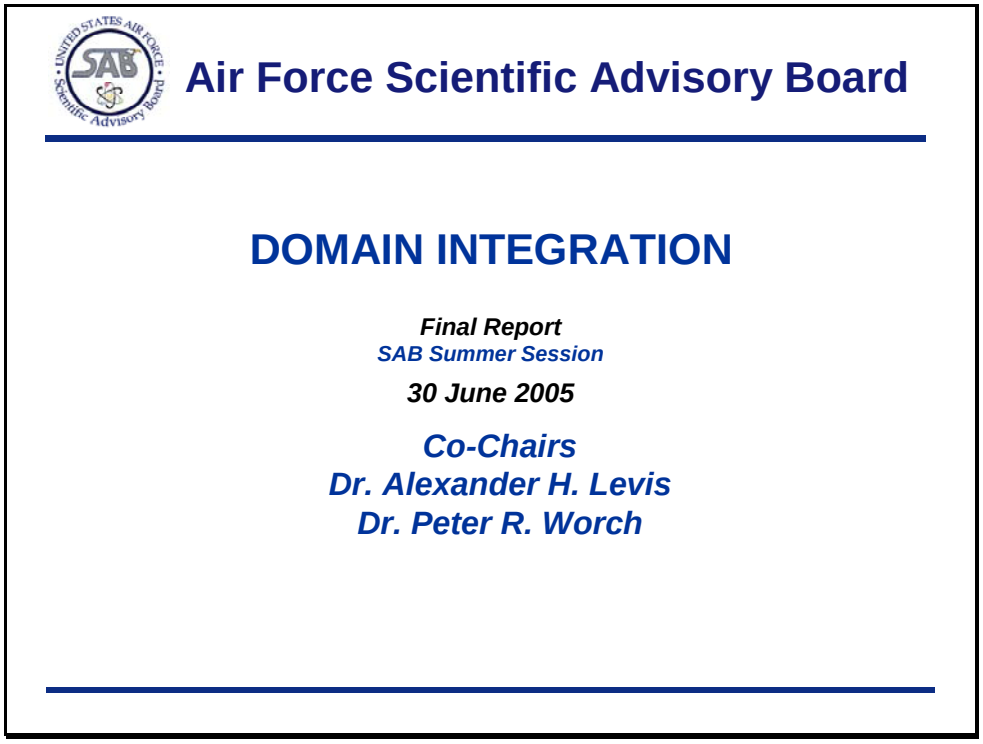
Recommendation 4. Experiment!

A dynamic process for injecting technical solutions to warfighter needs is critical to maintaining effectiveness of the Air Force. The standard process of formal requirements development followed by procurement is generally not capable of this dynamic action. Rather, a spiral process based on experimentation leading to fielding of incremental capability is recommended.

Summary

Interoperability is an achievable goal that should be approached principally through data integration, as contrasted with system integration. We recognize that there will be cases where system integration will be necessary to achieve a specific objective (performance, safety, and security are three such potential justifications).

To achieve this goal it is possible to start small and build incrementally, but it is very important to start with at least a critical mass (enough to get the process started and keep it running). Successful information integration efforts depend critically on elimination of barriers to information sharing across the enterprise.

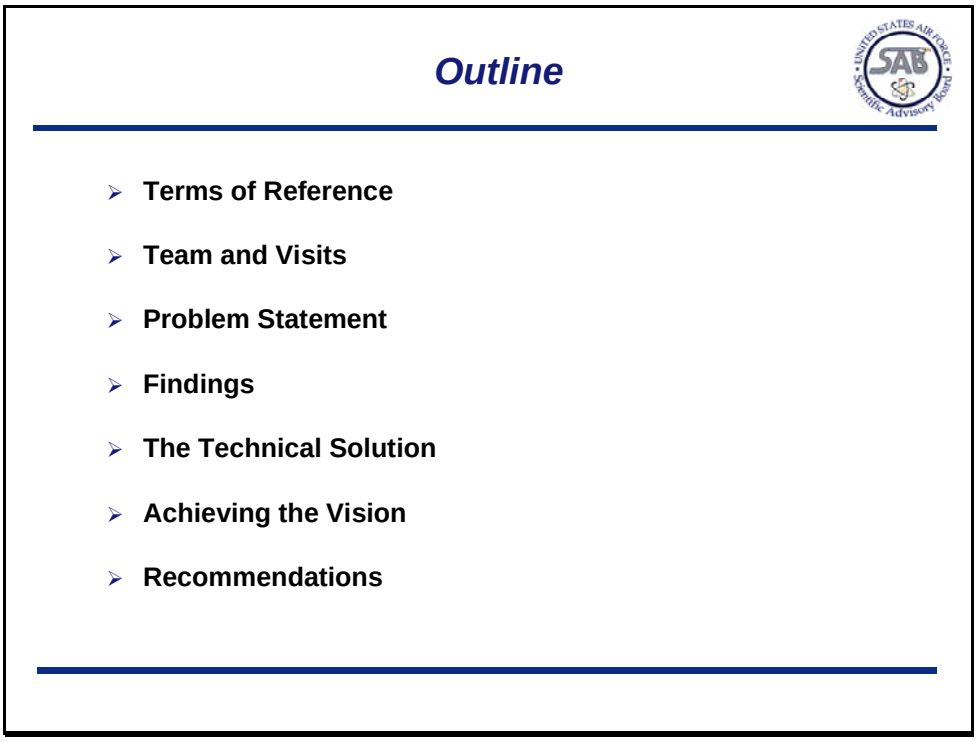


The Domain Integration Study was defined to be a complement to previous AF SAB studies dealing with the effective and rapid sharing of information among combat and combat support elements of the Air Force.

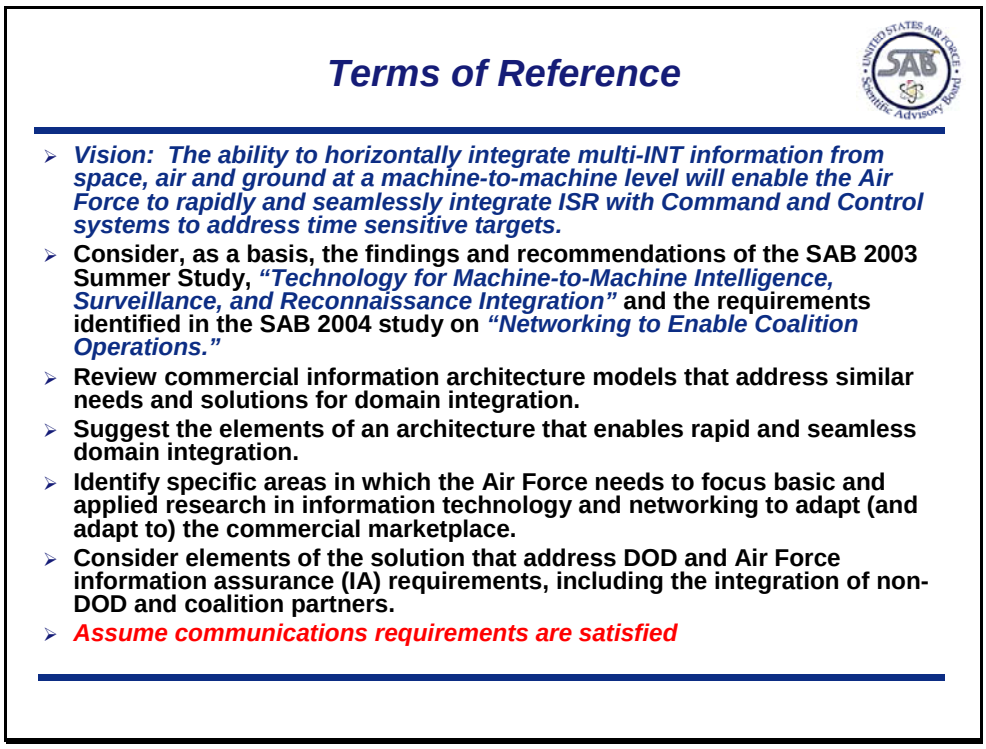
Co-Chairs:

Dr. Alexander H. Levis, George Mason University

Dr. Peter R. Worch, Private Consultant



This report provides the study background, proposes a specific technical solution to the problem, develops a vision of the future based on the proposed technical solution, and provides recommendations for actions to achieve the vision.

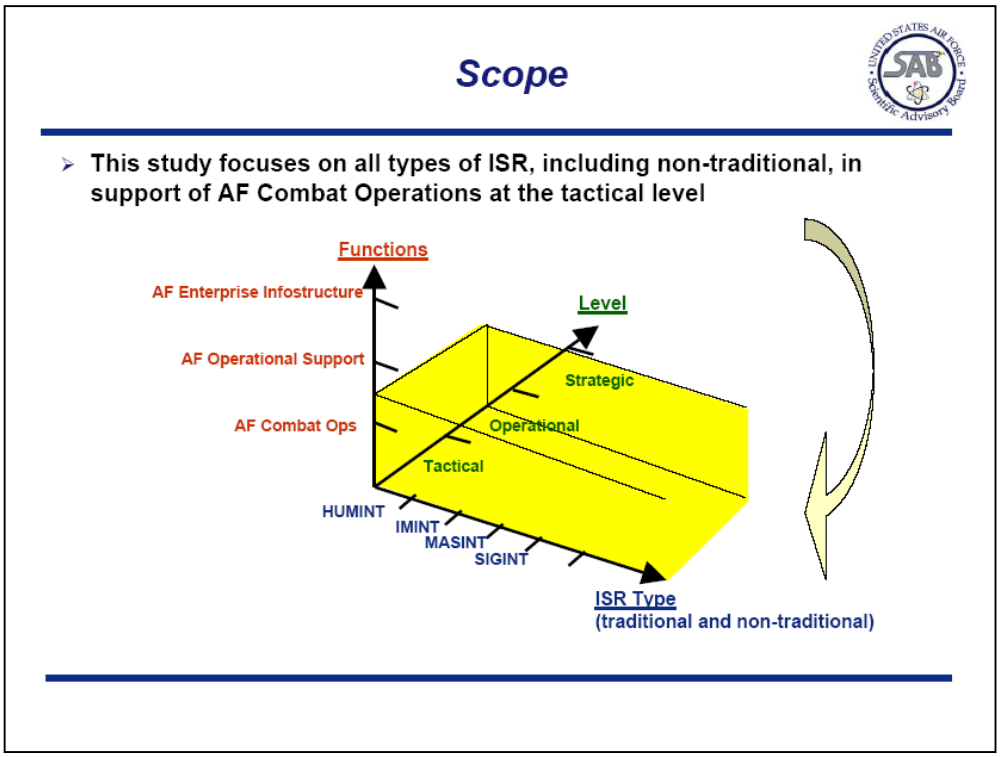


The Charter in the Terms of Reference (TOR) is shown here.

Of special importance is the vision presented at the top, in which we express the need to provide seamless information connectivity among warfighters engaging time-sensitive targets (TST).

The TORs draw attention to the substantial reference and dependence on two previous AF SAB studies:

- SAB 2003 Summer Study, *"Technology for Machine-to-Machine Intelligence, Surveillance, and Reconnaissance Integration"*
- SAB 2004 Summer Study, *"Networking to Enable Coalition Operations"*

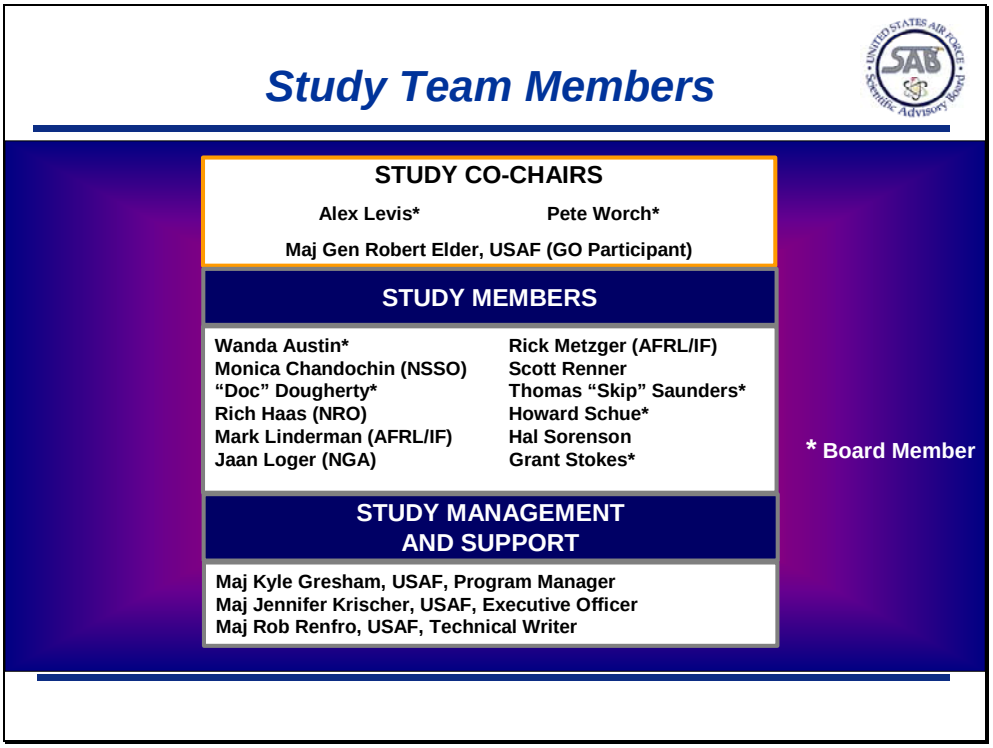


The notion of "domains" grew out of the 2003 SAB study on *Technology for Machine-to-Machine Intelligence, Surveillance, and Reconnaissance Integration* ("MTM study"). The MTM study observed that most ISR systems were driven to integrate (on a pair-wise basis) with a specific set of pre-existing systems that contributed to the mission of the sponsor or user.

These collections of capabilities and systems that fell under the effective control of a single organization or individual were labeled as "domains." Examples of identified domains included Intelligence (with sub-domains of imagery intelligence (IMINT), signals intelligence (SIGINT), human intelligence (HUMINT), and etc.), Combat Support, Combat Operations, Special Operations Forces, and etc. A byproduct of pair-wise integration was difficulty in moving information between systems that were developed to meet the needs of different domains.

This notion of "domains" extends readily to other axes of organizations (e.g., functions and levels) where RAAR continue to form the framework for investment decisions.

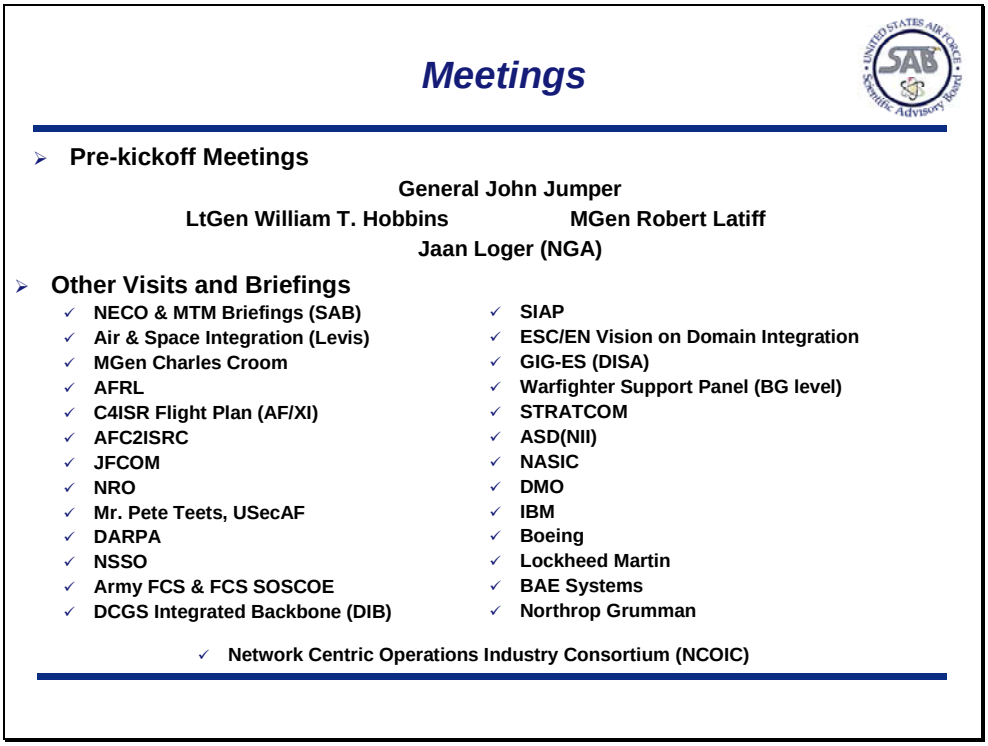
In a meeting with General Jumper, Chief of Staff of the Air Force (CSAF), the scope of the study was focused on combat operations, and especially on time-sensitive targeting using non-traditional ISR, at the tactical and operational levels. The latter included the relevant activities in a CAOC.



This study was extremely fortunate to have had the help of Major General Bob Elder as its General Officer participant. He brings the experience of his former role as Deputy Combined Forces Air Component Commander (DCFACC) for Operation Iraqi Freedom (OIF).

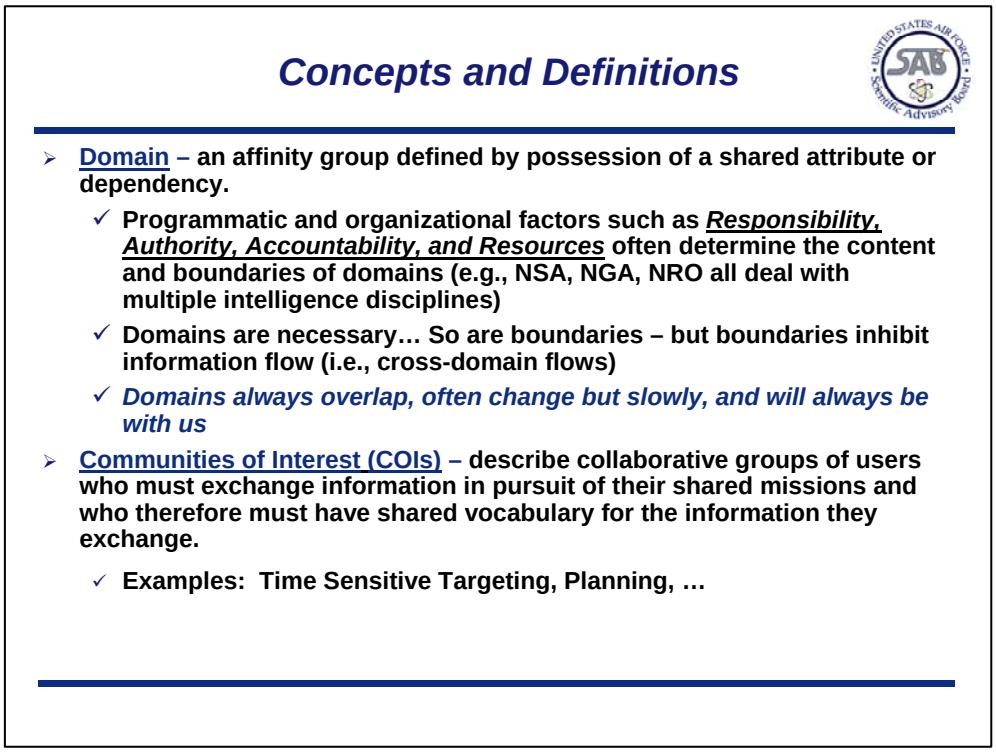
The study was also fortunate in being able to include important and knowledgeable experts from the Intelligence, Space, and Science and Technology communities to augment the knowledge base of the assigned SAB members.

Finally, we want to acknowledge the help of our study management and support team, as well as the SAB Secretariat and other staff assistants.



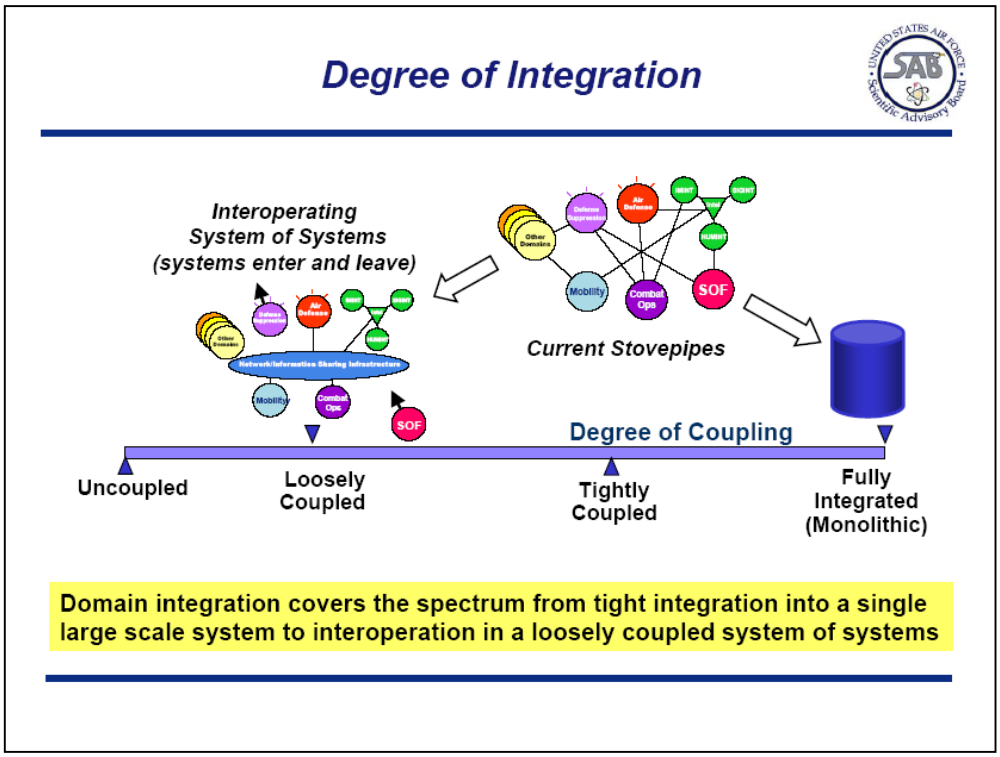
The Co-Chairs met with General Jumper (CSAF) to discuss the TORs prior to kickoff of the study. This meeting proved valuable in scoping the effort. They also met with Lieutenant General Hobbins (AF/XI – now SAF/XC), Major General Latiff, (NRO/DDSE), and Mr. Loger (NGA) to gain their perspective on the issue of Domain Integration. Mr. Teets, Air Force Undersecretary, also addressed the study team and provided guidance.

The study team received a large number of briefings from elements of DOD that contributed technically or operationally to the study's purpose. The group also discussed concepts and technologies with defense industry and, to a lesser extent, commercial industry.



A person or organization establishes domains, in general, to partition large undertakings into portions that can be credibly understood, controlled, and executed. This partitioning inevitably creates barriers at the domain boundaries with respect to architecture, infrastructure, information, and process. These barriers may allow efficient implementation within the domain, but impede tight integration with other domains.

The execution of missions often requires capabilities, information, and resources from multiple domains, which leads to the formation of COIs. According to the DOD *Net-Centric Data Strategy*, "COI is the inclusive term used to describe collaborative groups of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes and who therefore must have shared vocabulary for the information that they exchange." The COIs are formed or aggregated across domain or organizational boundaries and may be expedient or transient in response to emerging needs, or they may be long-lived or become institutional.



"Domain integration," is defined here as the implementation of (widely) shared functional interfaces between domains that allow (but do not necessarily require) access to, use, or control of resources and capabilities within the domains. In this definition, "integration" refers to a satisfactory degree of interoperation. Domains are integrated if the separate capabilities can work together without any "seams" that are observed by the warfighter. "Integration" also denotes a complete level of coupling. Coupling is a measure of the magnitude and cardinality of interdependencies between system elements. All systems that interact must be coupled to some degree. Tightly-coupled systems have many interdependencies; developer choices are largely constrained, such that changes in one system must often be reflected in all others. "Fully integrated" describes a monolithic system.

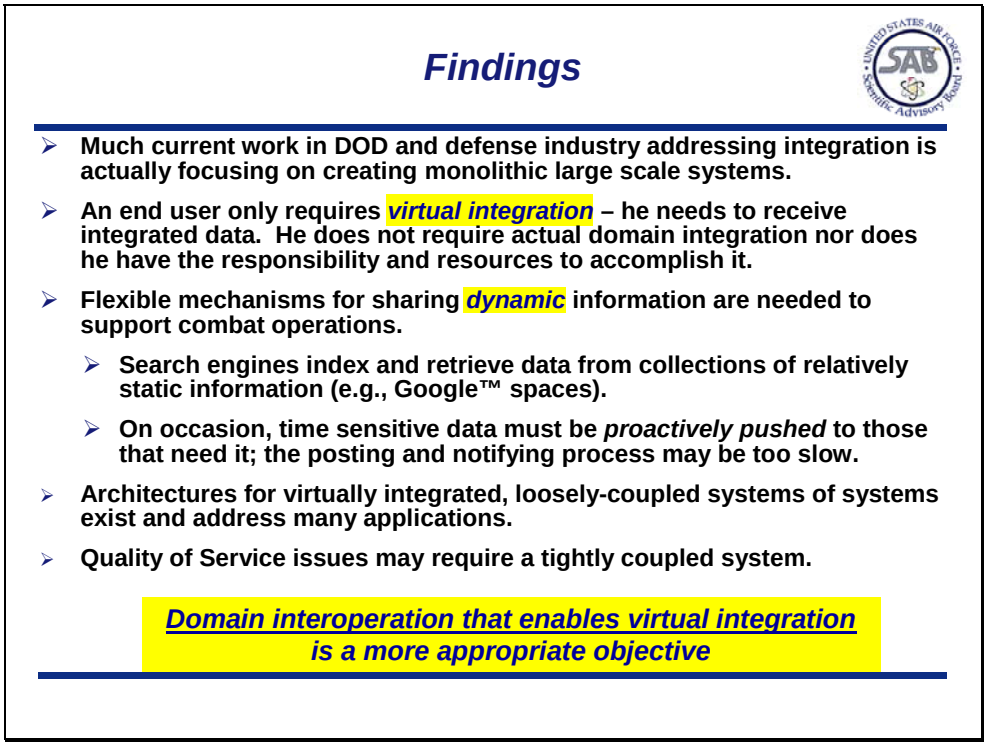
There are three aspects of domain integration:

1. Infrastructure integration: constraining the implementation choices of separate system builders so that data can be exchanged across system boundaries. In this dimension, tightly-coupled systems might be required to use the same hardware, operating system, and etc.; while loosely-coupled systems are required only to follow the standards essential to data exchange.

2. Information integration: constraining the data engineering choices of the separate data producers so that their data forms a single, coherent view of the world. In this dimension, tightly-coupled systems might all be required to internally implement a single, comprehensive data model; loosely-coupled systems are required only to interact with a simple interchange model. For example, the "Cursor-on-Target" (CoT) data exchange model requires agreement on only 14 key data elements (specifying the "what, where, and when" of battlefield entities).

3. Process integration: constraining the automated support provided to the separate operators so that their actions fit the expectations and needs of the mission-specific workflow. In this dimension loosely-coupled systems often rely on flexible information presentation (e.g., browsers) and support for collaboration and workflow.

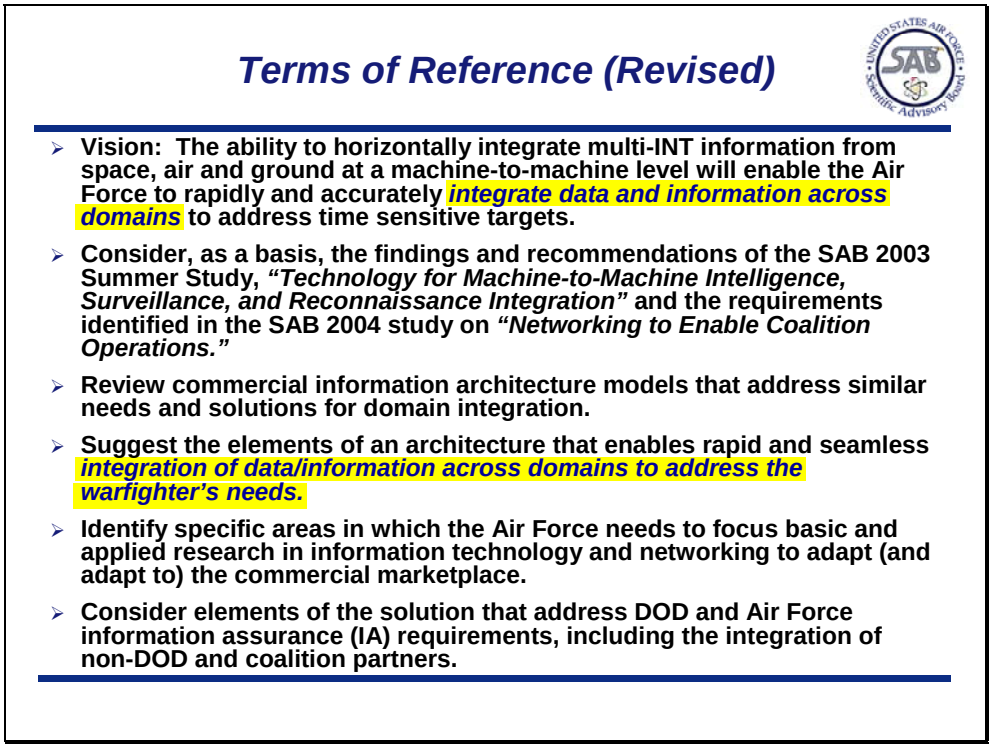
Domain integration can occur during any of the three phases of system evolution (requirements development, design/build, and operation). Agility and flexibility are greatly enhanced by the ability to integrate during operations ("last-minute integration").



"Integration" efforts are often aimed at producing completely coupled, fully-integrated system monoliths. These do not accommodate autonomy within the components in any aspect of integration (infrastructure, information, or process). Trying to satisfy the demands of users from multiple domains by following this approach is slow and expensive. The resulting system monolith is difficult to change.

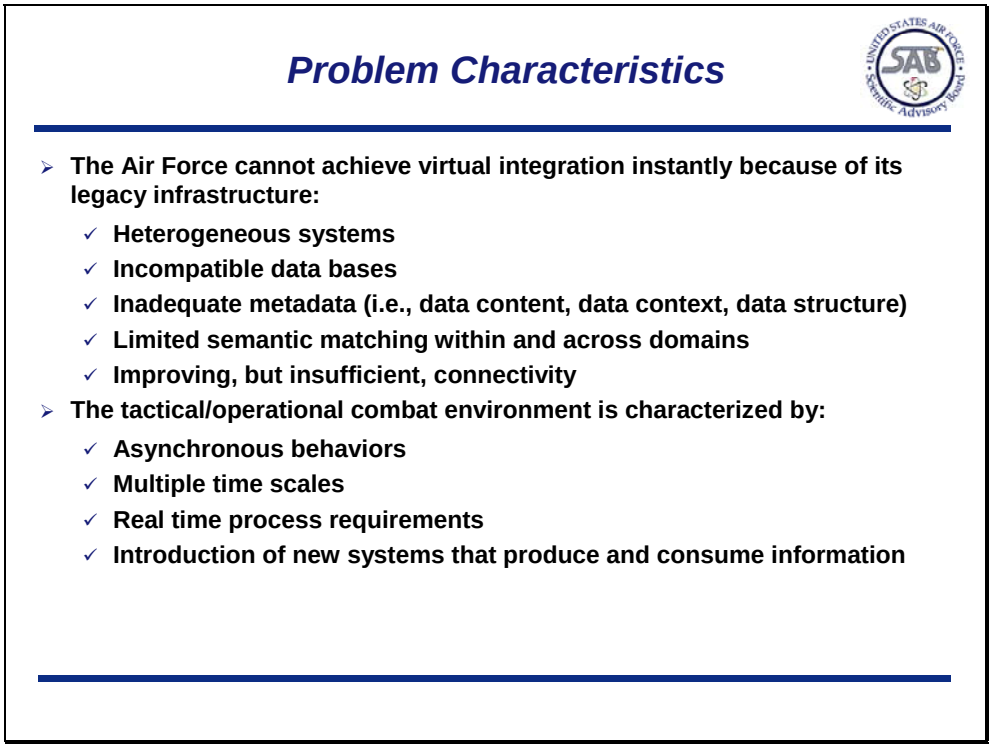
In some cases, creating a fully integrated system, such as the F/A-22 avionics system, is appropriate owing to requirements for performance, safety, and/or security.

However, the users do not care *how* their demands are satisfied. System monoliths are not required. All that is required is to make the right information available, machine-to-user *and* machine-to-machine. Very often the best (fastest, cheapest, most effective) way to achieve this is *not* to build an integrated monolith – instead, provide systems and information that can be quickly composed to satisfy changing needs. Domain interoperation, not (total) domain integration, is in general a more appropriate objective.



So, given the conceptual arguments for interoperability of domains only to the extent necessary to achieve integration of cross-domain data and information required to accomplish the mission, the modified version of our Terms of Reference above is provided for consideration.

Integration of domains is difficult and often very expensive, and may not necessarily lead to the desired end state even when successful. Thus, the Study Team advocates the *cross-domain integration of data and information* as a more appropriate objective for the Air Force. Subsequent findings and recommendations are offered in response to this modified study objective.

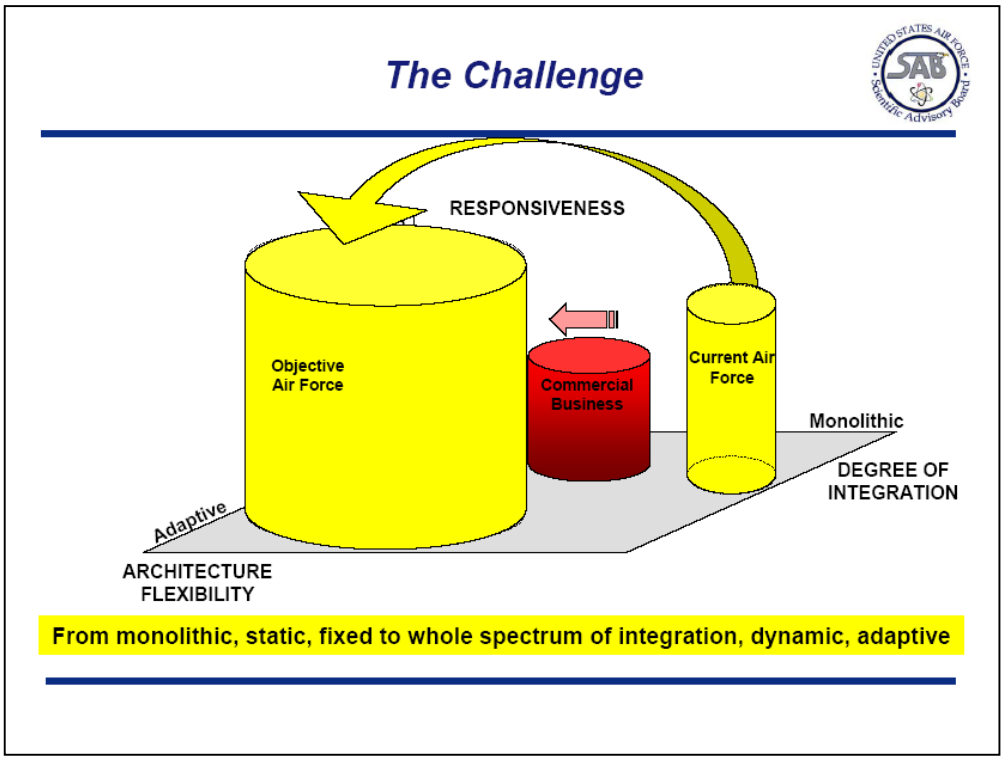


There is a high degree of heterogeneity and redundancy among organizations, processes, and systems. The history of the acquisition process is the production of legacy "stovepipe" systems, which have the characteristic that they were not planned and developed to work with most other systems in the overall national security environment. A critical problem in integrating these largely autonomous systems stems from inconsistent data/information models and associated databases. These inconsistencies lead to both syntactic and semantic confusion. The very difficult technical problem of "semantic matching," for example as addressed in the efforts in the World-Wide Web community directed toward the creation of the "Semantic Web," has some of the tools required to solve the problem. The problem, however, remains as a challenge to the general implementation of "virtual" integration.

Joint and coalition operations involve many diverse stakeholders with differing cultures and responsibilities. Stakeholder responsibilities often dictate very different time scales for their operation and the production of data, information, and products to be used by other elements of an operation. The accommodation of these multiple time scales presents an engineering challenge that domain interoperability must address and solve.

Joint and coalition operations need cross-domain interoperation that enables the ability to respond to unexpected events in a timely and effective manner. Events dictate that integrated systems must respond to asynchronous behaviors and demands. Further, the unexpected nature of events imposes the need for flexible adaptation supported by dynamic, sometimes real-time, composition of processes required to meet demands and produce effective, timely responses. Given the existence of ISR from traditional and non-traditional sources, the fusion of relevant data constitutes a cornerstone for understanding events and providing the situational awareness required for the response. Until these data are registered spatially and temporally on a common

basis, the fusion of the data cannot be accomplished effectively. Thus, semantic matching must be complemented by the timely registration of multiple types of ISR data. Then, decision support systems can be linked more closely to mission situations and events and, thereby, enable more timely and effective responses.

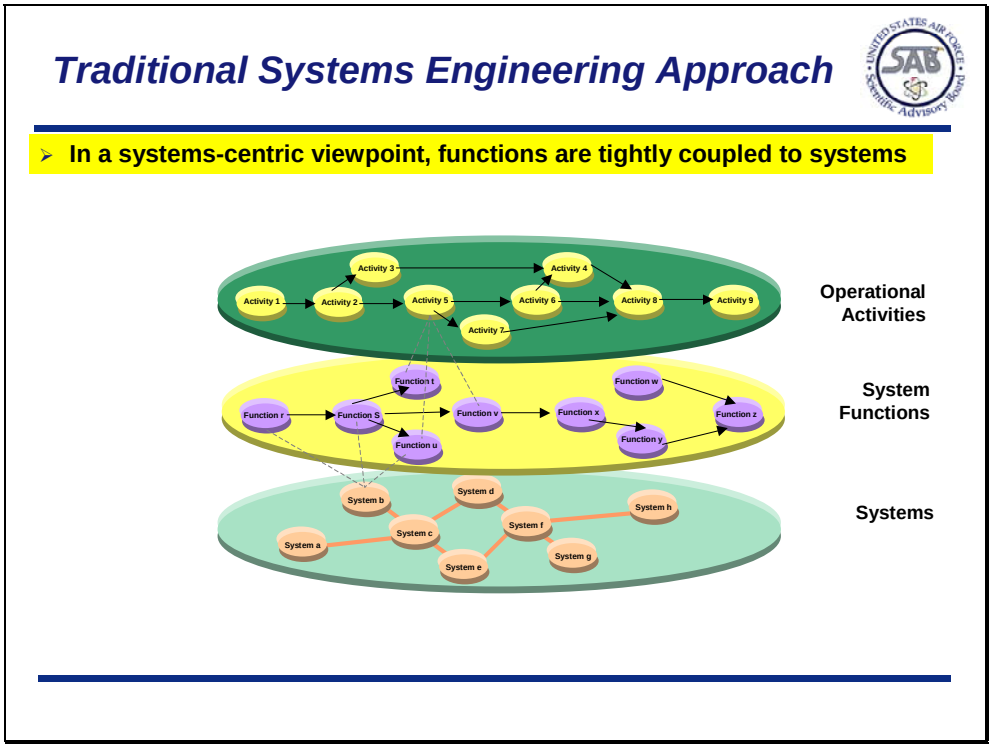


A challenge for the Air Force is to be able to immediately respond to unforeseen operational events discovered as a result of traditional or non-traditional sources of information from both internal and external means to the Air Force. As technology has advanced worldwide, our adversaries have been able to maneuver much more rapidly, thus creating a much more dynamic battlefield environment.

Historically, systems were monolithically integrated because of technological, programmatic, and cultural necessity. This resulted in pair-wise technical and operational interaction between elements of the force which, in turn, limited the ability to dynamically and adaptively respond to changes in the operational picture. The Air Force is structured such that interactions within the domains (stovepipes) and interactions across domains are restricted, and machine-to-machine interaction is largely precluded. Within the stovepipes the degree of integration is monolithic which results in a lack of flexibility and responsiveness to demands outside of the stovepipe.

Emerging technologies that enable machine-to-machine operations will allow an alternative approach to system development and operation. These technologies may be employed in a layered SOA, as proposed in this study. They will allow the Air Force to adaptively respond to the dynamics of today and tomorrow's battlefield. However, these emerging technologies discussed later in this report require significant and continued management emphasis, and programmatic support. Commercial industry has adopted the loosely-coupled notion for a number of applications (e.g., business-to-business supply chain) and is moving rapidly to expand the use of these ideas. Major hardware vendors have been moving aggressively in this area (e.g., IBM and Hewlett Packard).

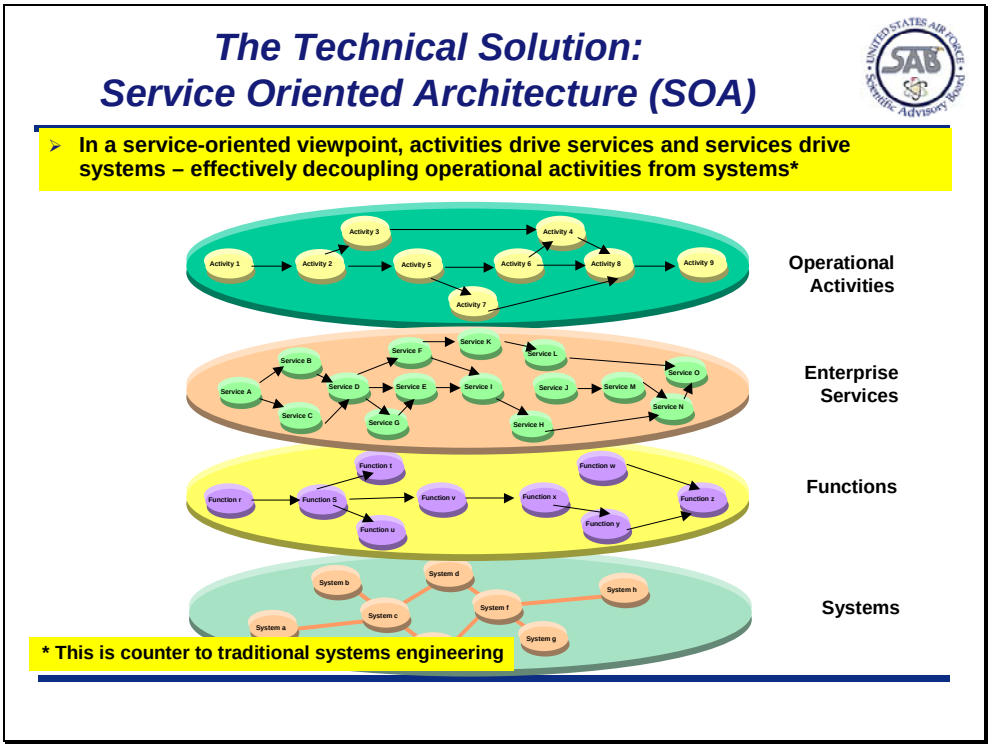
The objective is that the Air Force will span the spectrum of integration by being loosely-coupled as a baseline and integrated only where required. This maximizes the flexibility of the architecture to be dynamic and adapt to changes in the demands of the Communities of Interest. Domains can be added or deleted; COI's can be created or terminated; and the architecture is independent of the command and control structure (centralized or decentralized).



The Study's recommended approach for dealing with the complex problem of domain integration and interoperability is Service Oriented Architecture.

In the traditional systems engineering approach, operational activities are mapped to system functions that reside in systems. The assignment of operational activities to system functions is at the core of the design problem. The functions are then tightly-coupled with system-specific capabilities. The Air Force has routinely used this systems-centric viewpoint in the development of systems and domain-specific data sets.

An alternative approach has been developed to deal more effectively with the large number of extremely heterogeneous domains resident on the Internet. In this architecture, called Service Oriented Architecture internet-based services facilitate the creation of (Web) Communities of Interest to assemble and integrate data sources from multiple different domains in a manner consistent with the time, resource, and purpose-based needs of each COI.



In contrast, from a service-oriented viewpoint, operational activities drive services and services drive systems – thus, effectively *decoupling operations from systems.*

Briefly, **Service Oriented Architectures** is defined as: (1) an architectural style that encourages the creation of loosely-coupled mission services; loosely coupled services are interoperable and technology-agnostic thereby enabling mission flexibility; and (2) a solution consisting of a composite set of mission services that realize an end-to-end mission process; each service provides an interface-based service description to support flexible and dynamically composable processes. A "service" is defined as an application function packaged as a reusable component for use in a mission process. The service either provides information, or facilitates a change to mission data from one valid and consistent state to another. Re-use and composability are a key characteristic for any potential service.

The Service Oriented Architecture development is guided through satisfying the following requirements:

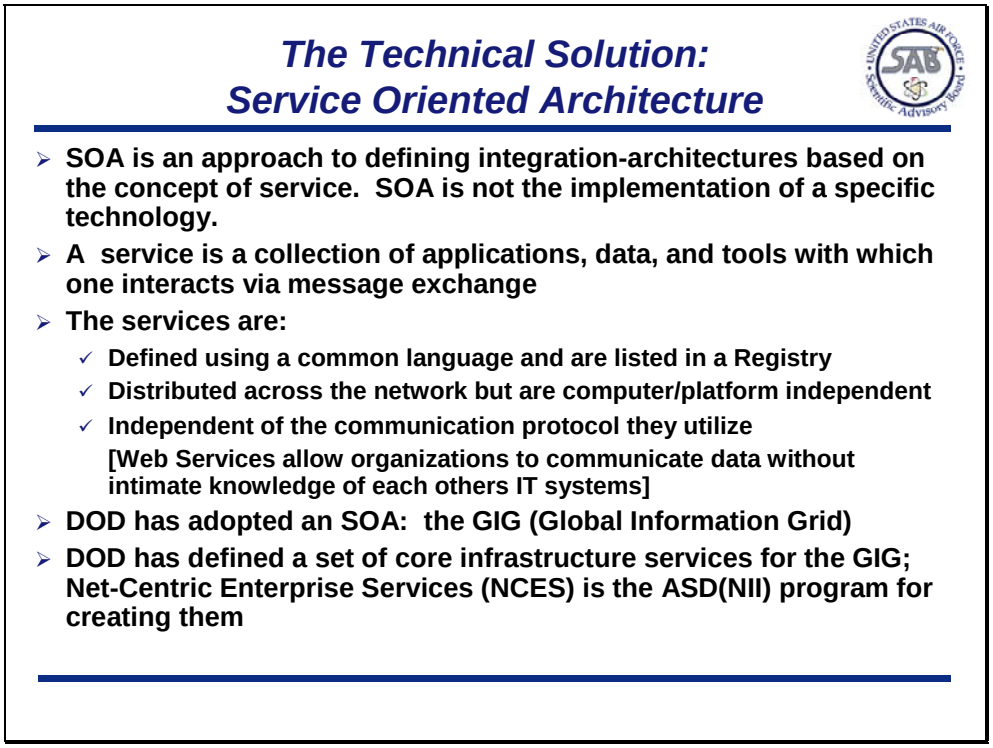
Simplicity, allowing efficient communication among disparate communities and stakeholders;

Flexibility and maintainability, not permitting local changes to impact the global system;

Reusability and composability, using services in more than one application or process and composing them to create mission processes;

Decoupling of functionality and technology, separating the long-lasting mission process and functions from the shorter life cycles of the underlying technologies. It is important to recognize at the outset that SOA is not an implementation technology.

An important driver for the use of SOAs stems from experiences that demonstrate that loose-coupling can be achieved without affecting the producers of the data / information in any essential way. Services are defined in terms of their interfaces and are separated from the service implementations. Their development is not an expensive or lengthy effort. Consequently, an SOA development incurs minimal cost, resource, and time overhead compared to fully integrated systems. It must be an AF-wide effort to implement only the necessary level of virtual integration.



These services facilitate the dynamic composition of multiple domain-specific datasets to support new missions, mission applications, or new information on time and resource scales consistent with mission requirements. To achieve the potential of a SOA, domain-specific datasets should be made both known to and accessible by the SOA, and have certain consistent descriptors (metadata) that characterize the data in such a way as to allow the SOA to properly handle and characterize them.

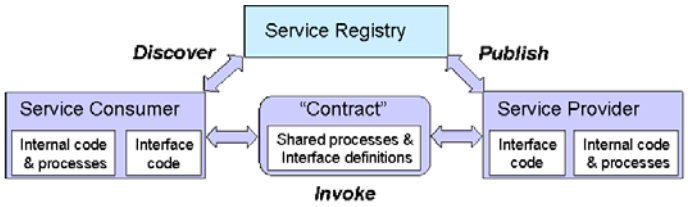
The service descriptors are included in a service registry. The SOA provides the mechanisms for communicating and discovering services as a first step toward invocation of the services to create a needed process. The capability to dynamically compose end-to-end processes for new or altered missions provides the flexibility to respond effectively to unplanned or unexpected events. In support of the process implementation, an SOA provides a service bus. The service bus provides the interconnectivity services that allow services to interact with each other based on the Quality of Service (QoS) requirements of individual transactions. It must support synchronous/asynchronous and persistent/non-persistent behaviors and the interoperation of loosely-coupled/tightly-coupled services and applications across heterogeneous platforms, environments, and transport devices. Through the use of bus services (e.g., mediation, transformation, and routing), the service bus enables transparent support of user/operator requests and requirements. The service bus is based on World Wide Web standards and commercially available services (e.g., web services).

Web services serve as key building blocks for an SOA. In addition, the nine services planned for the GIG ES provide another building block for the SOA. DOD has adopted the SOA approach in its development of the Global Information Grid. Specifically, the DOD has identified nine specific services that the GIG will offer to subscribers, and the GIG program

called Net-Centric Enterprise Services is charged with the development and provision of these Services to GIG users.

Domain Interoperation via SOA

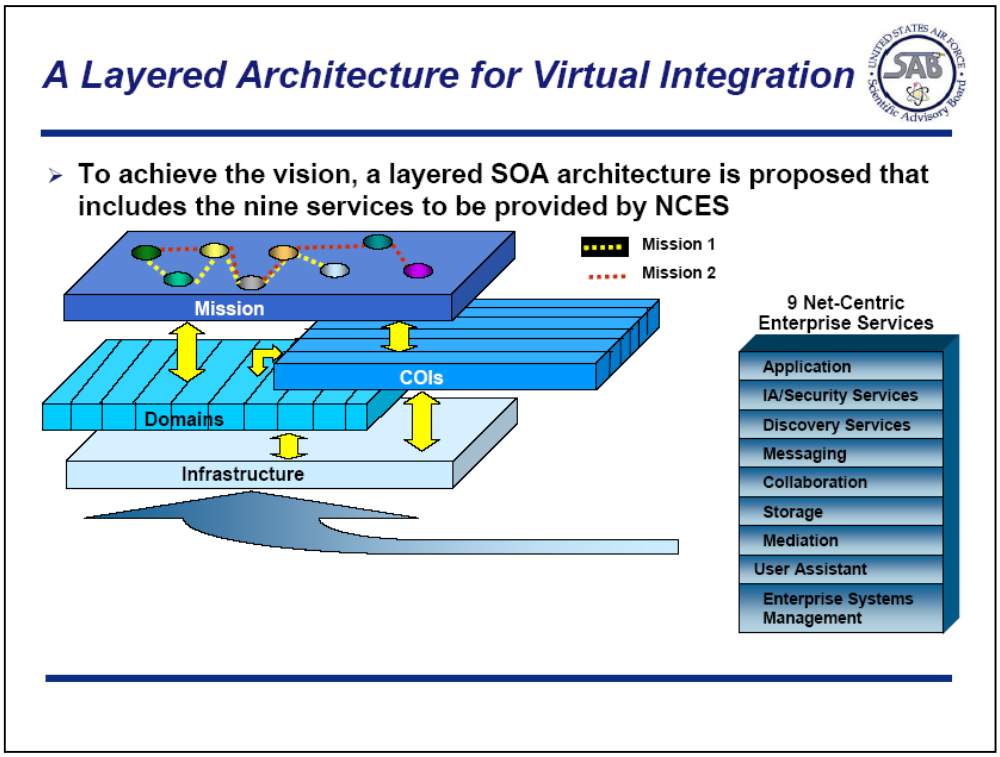
- **SOA provides domain interoperation (loose-coupling) by defining elements as service consumers and service providers/publishers.**
- **When consumers discover a service, they bind to the service through a published standard interface mechanism and a contract is established.**
- **For every domain, consumers can**
  - ✓ **Consume any number of services and**
  - ✓ **Compose existing and newly developed services and publish as another service**



The "Cursor on Target" schema is an instantiation of loose-coupling for information exchange.

Service consumers, or users, make their needs known by querying a registry of SOA services using a *discovery* process. When the consumer discovers the appropriate services, he *invokes* a contract with the service provider using standard processes. The service provider then provides the relevant service to the consumer using a *publish* process, which runs through the service registry so other consumers become aware of the specific, new *discovery-publish* relationship that has been established.

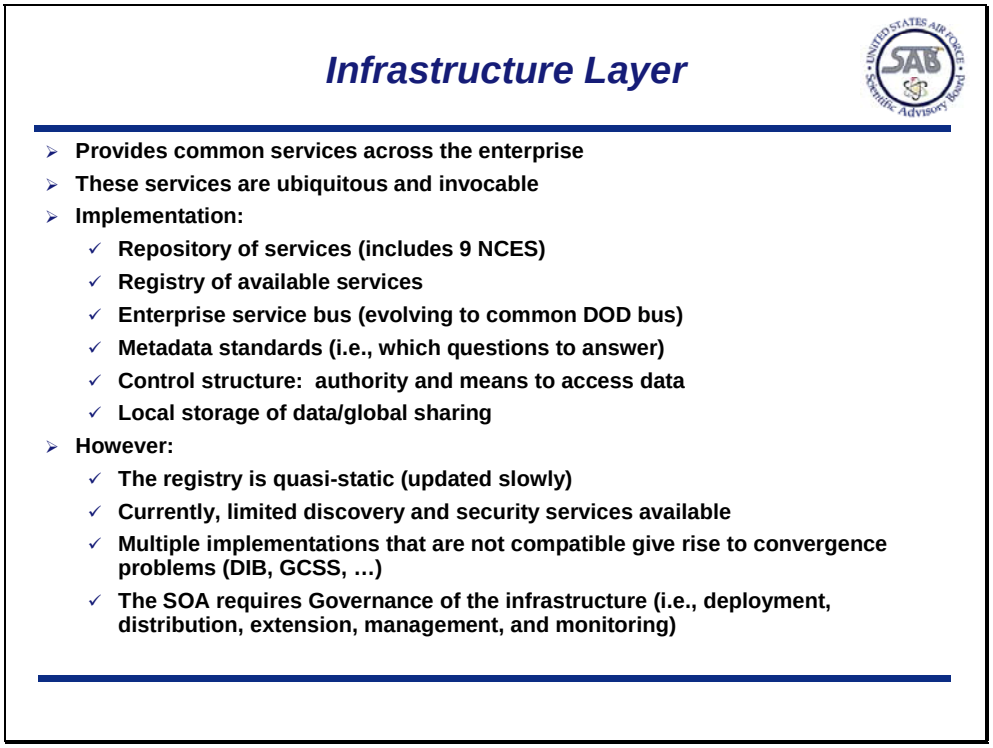
An SOA development is generally characterized by "*I can't tell you what I want, but I will recognize it when I see it.*" In this context, a successful development must be driven by the need to provide frequent delivery of useful capabilities. It begins by defining the "process" through which a mission is executed (i.e., thereby defining a "mission thread"). The "services" that are required to execute the mission are identified along with the service interfaces (i.e., the data/information required to use the service). These service descriptions are added to the service registry to enable them to be communicated and/or discovered by potential users. Then, the required capabilities of the service bus are identified. If the existing form of the service bus already includes required capabilities, plans for their use are determined. Otherwise, the service bus is augmented for use by the mission thread and for future applications. The service bus provides interconnectivity services**.** The SOA development is accomplished in a spiral manner and the SOA capability is allowed to evolve as the range of missions that may be supported grows.



To ensure that the domain interoperation SOA concept is logically organized and comprehensively addresses all the dynamic aspects of Air Force operations, it is necessary to formulate an architectural construct. The most appropriate approach for the problem studied is a four-layered, non-hierarchical architecture. This architecture assumes that the essential unified communications and network foundation is available. The remaining functionality is then divided into infrastructure, domain, COI, and mission layers that support the interactions across and between all elements of the identified layers.

The infrastructure layer forms the foundation of the architecture and includes the "core services," common to all layers, and a registry of layer-unique services. Although these core services have not been fully developed, ongoing efforts in the DOD and USAF have identified the appropriate, initial nine core services, and they require continued support. In addition to these core services, the elements of the domain and COI layers will create services to support functions within their layer. These services are also registered by the infrastructure's "discovery" service so that others may draw on them as required. At this time, the Net-Centric Enterprise Services program has defined nine services.

The dynamic combination or recombinations of the various services discovering and manipulating the data within the architecture provide the necessary functionality to meet mission needs.



The infrastructure provides the essential common support to all the SOA elements. Although the NCES program plans to provide nine core services eventually, only two are partially developed: discovery and security. The *discovery* service will provide visibility and access to information. While the *security* service provides information assurance capabilities that are commonly required across the architecture to consistently manage security, it does not provide all the necessary security functionality. Much of that functionality is provided by the service providers in the domain and COI layers as defined by the missions they are created to support.

The other services in the infrastructure are: *enterprise management* service that provides end-to-end operational management of the infrastructure; *messaging*, *collaboration*, *mediation* provide, along with *discovery*, comprehensive access to information; *application* provides protected operational hosting environments; *storage* provides data storage and retrieval of all data by all authorized users; and *user assistance* provides automated user support to decrease manpower intensive tasks.

Since the infrastructure layer forms the foundation for mission success, end-to-end management of the infrastructure is critical. Thus it must be planned, built, sized, implemented, operated, and managed carefully to ensure that operational needs are met. Therefore, an effective process must be developed to ensure that the appropriate governance is in place to support the development and deployment of the SOA infrastructure. There is a relatively nascent process in place today that will evolve over time. The process being pursued by the Network Centric Operations Industry Consortium (NCOIC) provides a model to enhance existing processes so that the various service providers can effectively govern the effort while still ensuring seamless interoperability.

Domain and COI Layers

COIs / Domains	Targeting	2	3	4	5
Combat Ops	X		X	X	
Intel	X	X			X
SOF		X	X		

- **Domains produce the data and evolve slowly**
- **Domains and COIs add metadata to their products**
  - ✓ **However, domains are metadata tagging only sporadically in spite of policy**
- **Domains and COIs generate services**
  - ✓ **All services are registered and available to other domains and COIs**
- **COIs compose processes from services and execute them**
  - ✓ **Metadata and registered services allow responsive product generation**

In a net-centric system, domains and COIs form a symbiotic pair: domains allow partition of the problem into pieces that can be managed and implemented and COIs aggregate information across domains to solve a particular mission problem.

Domains, since they tend to represent data producing systems, are generally longer lasting and evolve more slowly than COIs, which may be composed and evolve dynamically in response to changing needs. Both domains and COIs should produce comprehensive metadata which documents their output. Metadata is a key component of net-centric systems, the existence of which allows other domains and COIs to understand and directly use information products discovered on the network (i.e., the products are self documenting). Unfortunately to date, and in spite of specific Air Force policy (i.e., *Air Force Information and Data Management Strategy*), domains in the Air Force are not generally producing comprehensive metadata for their products.

Another key tenant of the net-centric strategy is that both domains and COIs register and post services that they have developed so that other domains and COIs may use them. For example, a domain that produces a specific data stream may post the calibration services needed to convert the data to engineering units, while a COI may post a target detection algorithm as a service for the same data. Thus, the COIs which compose processes intended to solve specific needs may make use of the services generated by any other COI or domain, which accrues substantial advantages with respect to response time and efficiency.

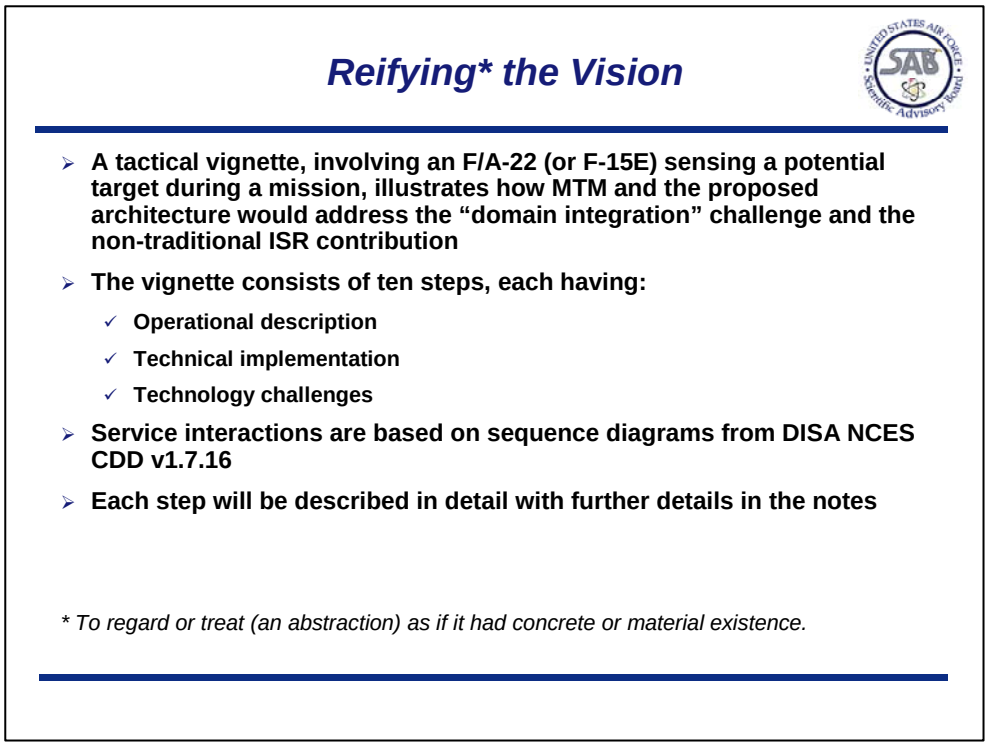
Remarks

- A notional architecture for interconnecting domains has been identified (2003 MTM)
- A rule-based, role-based approach to data access has been recommended (2004 NECO)
- Both studies identified the critical role of metadata
- In this study, the technical solution is identified
  - ✓ It can be done
  - ✓ It can be done incrementally, but it won't work unless all pieces are done to some extent
- The "what to do" is known
  - ✓ Add metadata (data content, data context, data structure)
  - ✓ Implement Service Oriented Architecture
- The "how to make it happen" in the Air Force is challenging
  - ✓ Institutional barriers
  - ✓ Not enough people trained to think this way especially in positions that can make a difference

This study builds upon the concepts and recommendations offered in the 2003 and 2004 SAB studies cited earlier, which describe a technical solution to the automated machine-to-machine domain integration problem. That technical solution is based on two fundamental premises – the availability of metadata and the employment of Service Oriented Architecture.

The availability of metadata (i.e., data tied to the basic data set that describes the content, context, and structure of the basic dataset) is critical to achieving any sort of automated machine-to-machine cross-domain interoperability. This is because information contained in the metadata is needed by any process using data from more than one domain to reconcile the datasets with each other and extract new insights from the combined information.

The employment of the Service Oriented Architecture incorporated in the GIG, as described on the preceding pages, is the second fundamental premise. Although the Study Team believes its proposed technical solution will work and can be applied incrementally, unless all aspects of the solution are undertaken, at least to some extent, it is likely that the Air Force will not ever achieve a satisfactory end state. For a chain to be functional, every link needs to be present and connected. This will be demonstrated in the illustrative example of how to achieve the vision. In other words, unless sufficient Responsibility, Authority, Accountability, and Resources are assigned to each element of this task in a coordinated fashion, then it is likely to fail. Thus, it is incumbent on senior Air Force management to ensure that sufficient RAAR is assigned and applied appropriately.



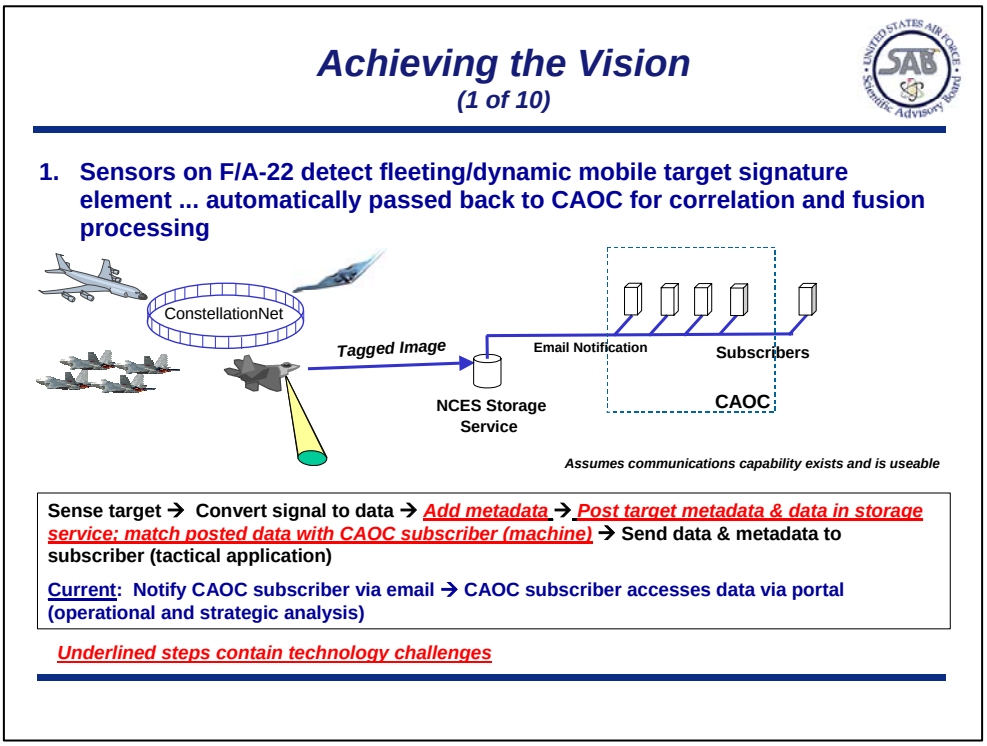
The 2003 Machine-to-Machine ISR Integration study concluded that the lack of a common architectural framework was a major factor inhibiting broad implementation of machine-to-machine communications and recommended that the Air Force:

> Define and build a modern technical architecture and its associated information services-based infrastructure. This report continues to advocate this path and proposes a specific Service Oriented Architecture.
>
> Institute enterprise data management in each of the Air Force's major domains to include assuring semantic agreement, a metadata registry, and explicit data ownership/sharing. This process has started, but is not a major focus of attention or consumer of resources.
>
> Develop data management across domains. This is in process by the Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer (ASD(NII)/DOD CIO).
>
> Incorporate responsive access to non-traditional sources as part of ISR operations integration to include tactical aircraft early warning receivers and synthetic aperture radar imagery, and weapon sensors. This initiative could make substantial contributions to shortening the effects chain timeline.

However, it is important to test the applicability of this proposed approach to the challenging domain integration problems the Air Force faces, especially at the tactical level. For example, we must determine: whether this approach sustains the rigorous objectives of "Cursor on Target;" whether an SOA approach is adequate to support the many and varied time-critical needs of operational planning and execution in the CAOC; and whether the impediments to

domain integration (e.g., security constraints) imposed by data owners and limitations of the domain-specific data sets can be effectively overcome using this architecture approach.

In the initial direction, we were provided a specific problem, expressed in the form of a mission vignette. This vignette, in an expanded form was adopted as the basis for assessing current shortfalls and defining the steps, with associated technologies, which would move the information in a machine-to-machine architecture. The following pages will examine the applicability and character of such an approach, and uses the stressing F/A-22 vignette to test the proposed approach's viability.

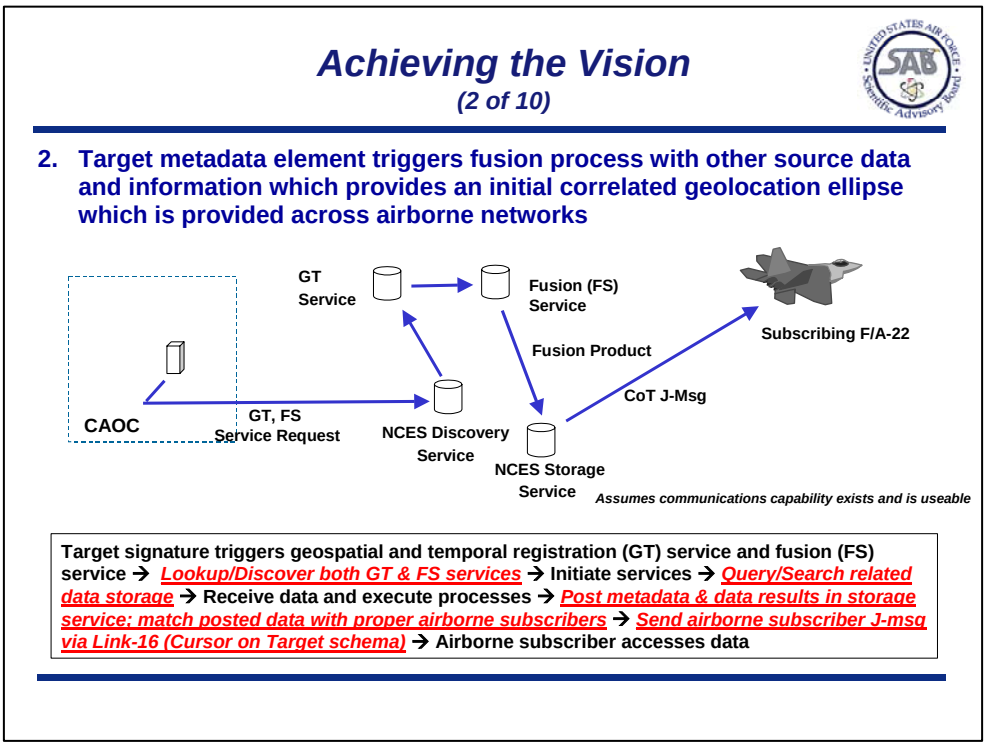


Step 1. Some of the steps occur before the F/A-22 detects the target. Application programmers and end users contact the discovery service and search for services that produce the information they need. Programmers look for machine-to-machine inputs to their software; end users look for information they can examine through browsers or other presentation software. When useful services are found, the applications register subscriptions to the desired information, via the Messaging service. These subscription requests are validated by the security service and an acknowledgement of the subscription is returned. At this point, a set of applications as well as CAOC users are prepared to receive information directly or be notified by the SOA when information of the type they are subscribing to exists in the information space.

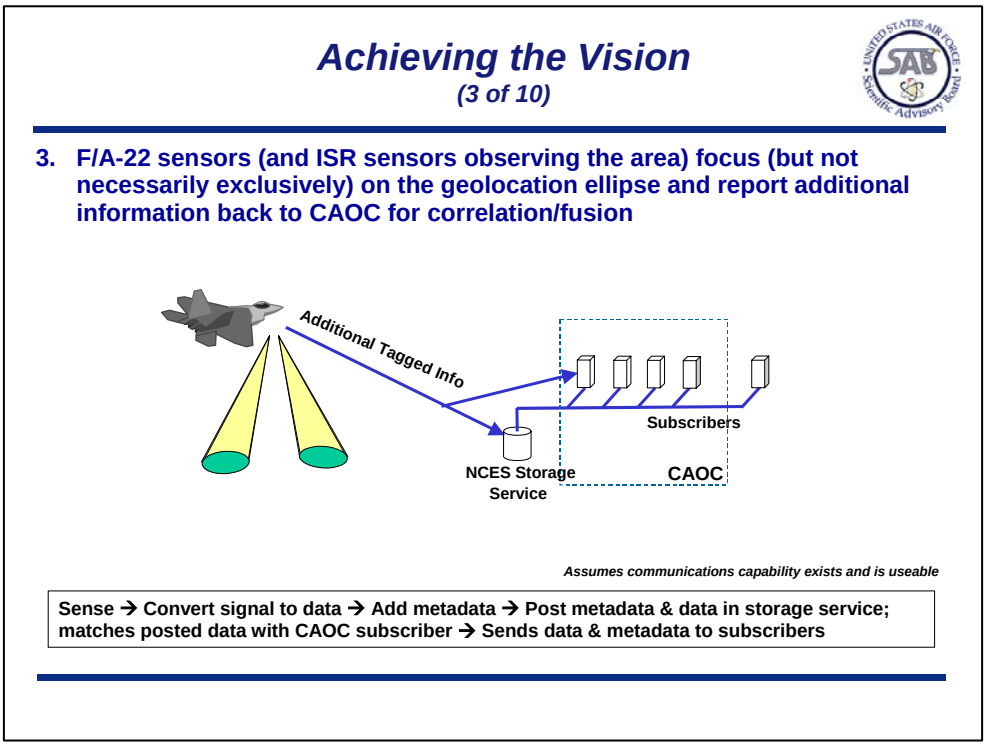
The F/A-22 is now airborne and during the course of its mission detects a fleeting target and collects data on that target with its onboard sensor. The sensor data is marked up with XML metadata at the sensor and is prepared for posting to the GIG. As the data is marked up, the F/A-22 makes a request to the NCES storage service to post the newly collected marked up data for sharing amongst the necessary applications and human users. The NCES storage service receives this request and forwards an authentication request to the security service to authenticate the F/A-22. The security service validates the F/A-22 and returns the validation authorization to the storage service which stores the marked up target data.

As the marked up data is stored, the storage service triggers a notification signal to the messaging service indicating that new target information from F/A-22 exists. The messaging service brokers this notification of new F/A-22 target information across all the existing registered subscriptions for this information. The messaging service sends a message to all registered subscribers (applications) that new target information exists. The application now contacts the storage service to retrieve the new target information for processing. In parallel, the

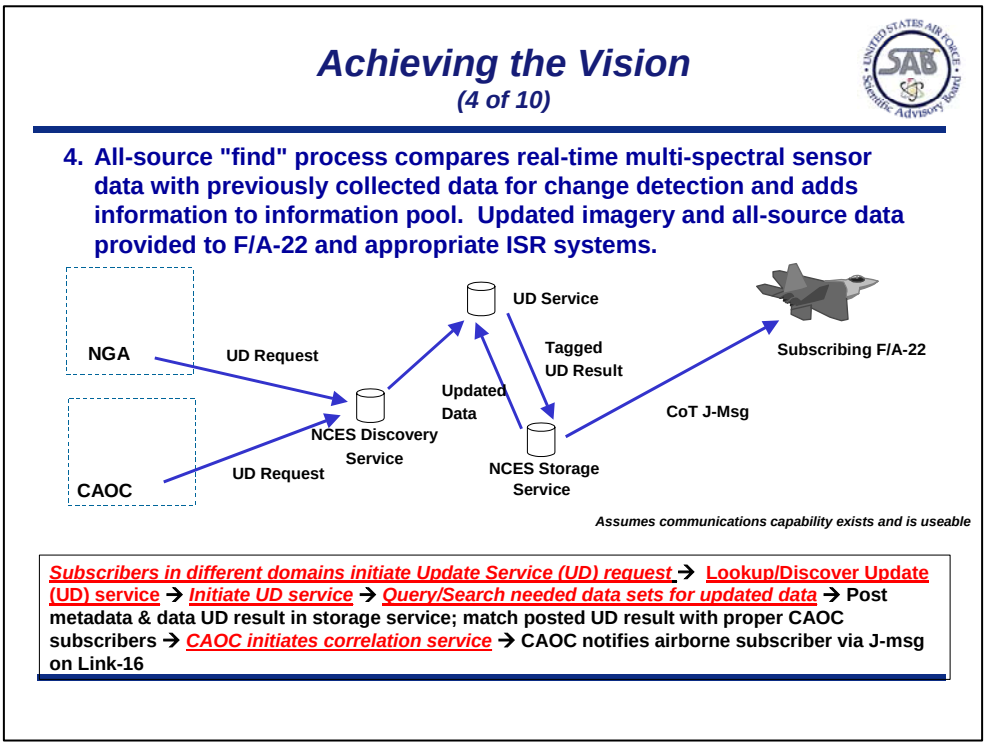
messaging service formats and sends an email to all registered CAOC subscribers (human) that new target data from an F/A-22 exists that matches their subscription predicates. Via a portal, the CAOC users can click on the URL within the email message, triggering a request to the storage service to retrieve the new F/A-22 data.



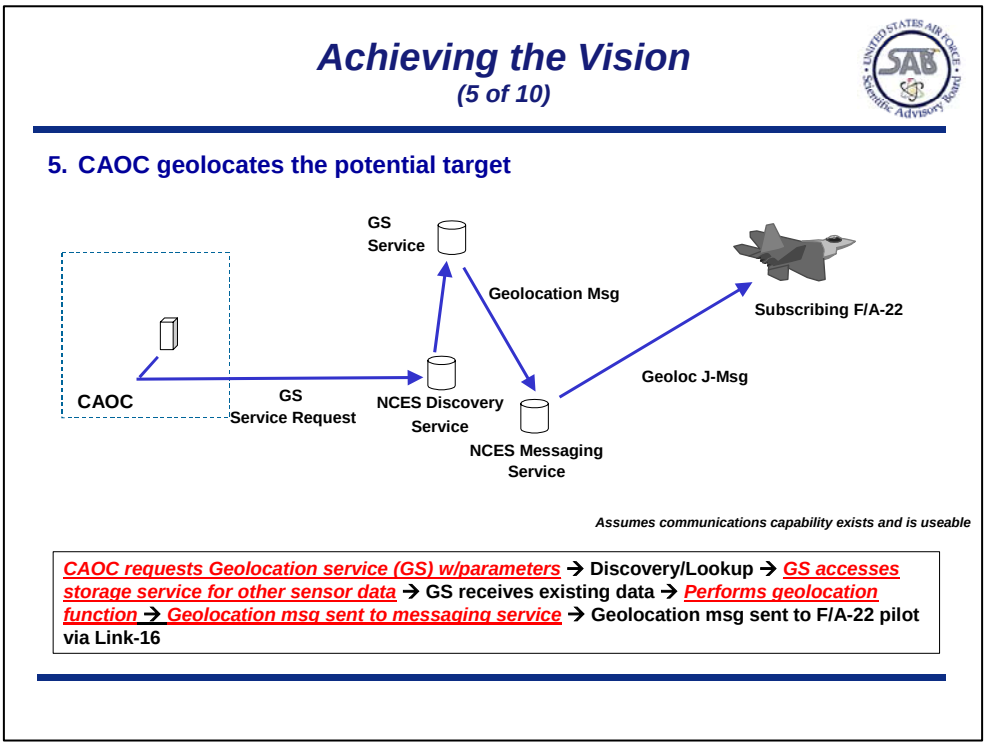
Step 2. After receiving the target signature from the storage service, the CAOC user initiates a request for geospatial and temporal registration, along with fusing the incoming target data. The initiated service request triggers the discovery service to locate the Geospatial and Temporal Registration (GTR) service along with the fusion service. The proper services are located and initiated. The CAOC user requesting the service is authenticated via the security service and the service execution proceeds. The GTR and fusion service, in parallel, query the enterprise storage for all the relevant target data and supporting data and compute the registration and then fuse all results. The resulting data is marked up with XML metadata and is posted in the storage service and alerts the messaging service that new data exists. The messaging service matches the posted stored service results with the proper airborne subscribers whose subscription predicates match the new data, formats a new message with the resulting data and sends it in a Cursor on Target schema over Link-16 to the subscribing F/A-22.



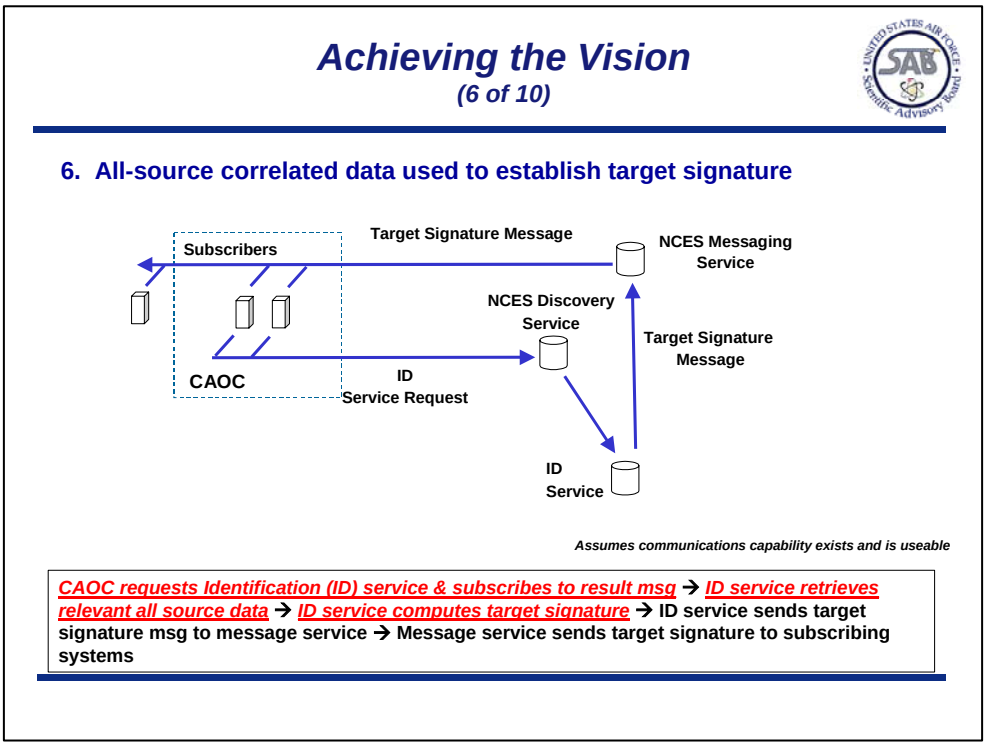
Step 3. The F/A-22 is now focusing on an area based on the new registered and fused results it just received. It collects new data for further registration and fusion. The new sensor data is marked up with metadata at the sensor for posting to the GIG. As the data is marked up, the F/A-22 makes a request to the NCES storage service to post the newly collected marked up data for sharing amongst the necessary applications and human users. The next steps are identical to those in Step 1. Again, via a portal, the CAOC users can click on the URL within the email message triggering a request to the storage service to retrieve the new F/A-22 data.



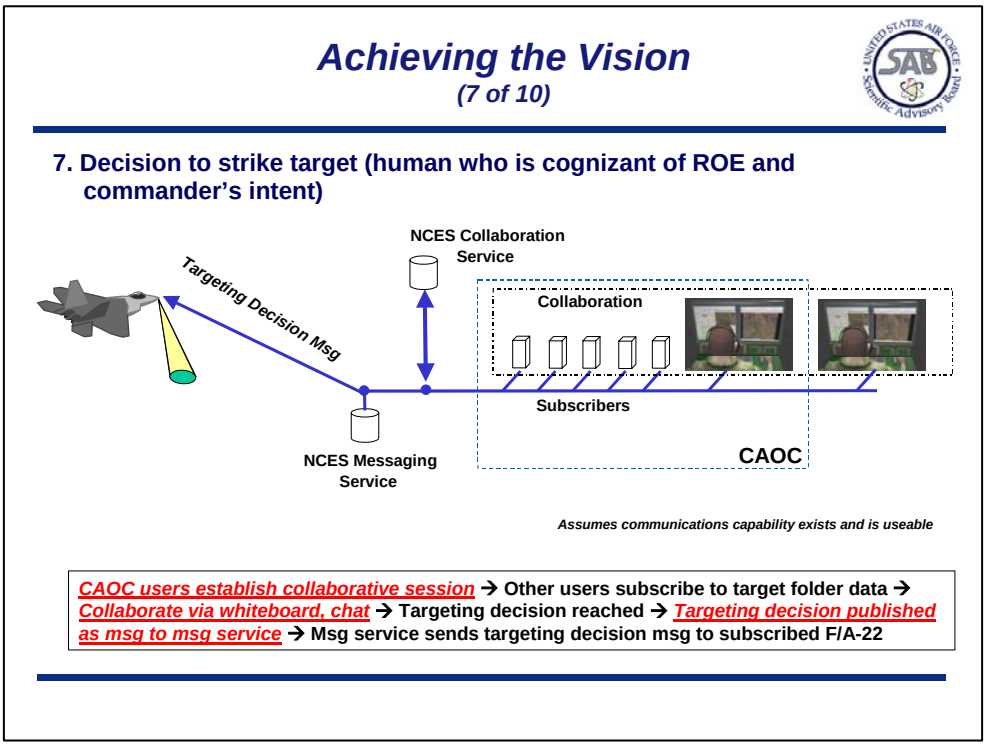
Step 4. As new marked up data comes in from the F/A-22, subscribers in several different domains receive notification that new F/A-22 data exists. These users initiate an update service that gathers the new F/A-22 data as well as other relevant data. The new data is posted to the storage service that matches the new data with subscribed CAOC users. These CAOC users initiate a correlation service. The correlation service correlates the new data and posts results that are sent to authorized airborne subscribers including the F/A-22.



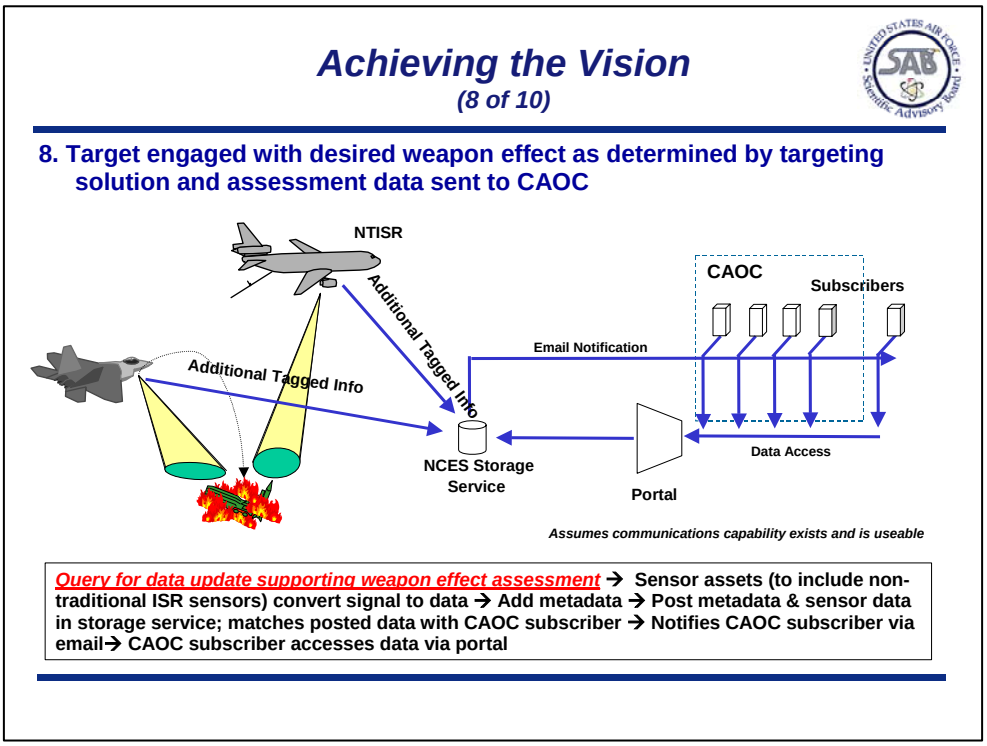
Step 5. As a result of the correlated data, the CAOC user requests the Geolocation Service (GS) via a Portal with the new parameters it has received from the F/A-22. The NCES information assurance (IA)/Security service authenticates the CAOC user and triggers the NCES Discovery service to locate the GS in the GIG and initiates the Geolocation service with the new parameters. The GS service computes the geolocation and automatically sends a geolocation message to the NCES Messaging service. The Messaging service matches up subscribers (F/A-22) to this geolocation message and publishes the message to those subscribers.



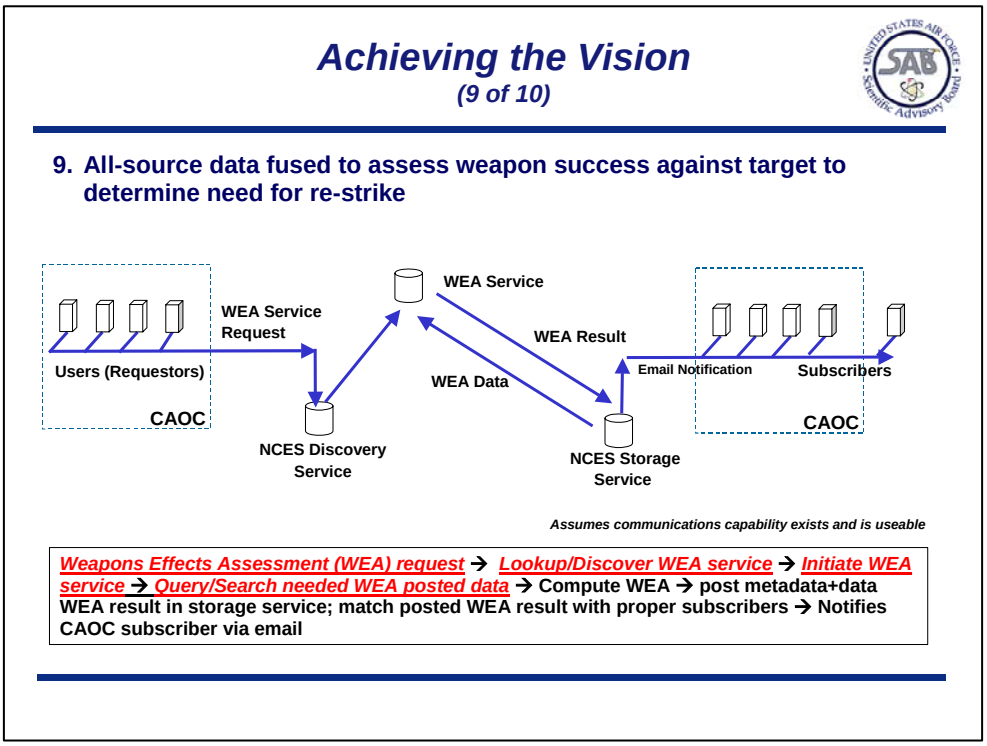
Step 6. Via the portal, the CAOC user requests the identification service (ID) to establish the target signature based on the F/A-22 data. The NCES IA/Security service authenticates the CAOC user and passes the ID service request to the NCES Discovery service, which locates the ID service in the GIG and initiates the Geolocation service with the new parameters. The ID service takes the F/A-22 data and signals the storage service to retrieve all relevant all-source data to compute the identification. The ID service takes in all this data and computes the target signature and sends a message with the result to the NCES Messaging service. The messaging service matches all subscribing systems, which include machine interfaces and human users both within and outside the CAOC.



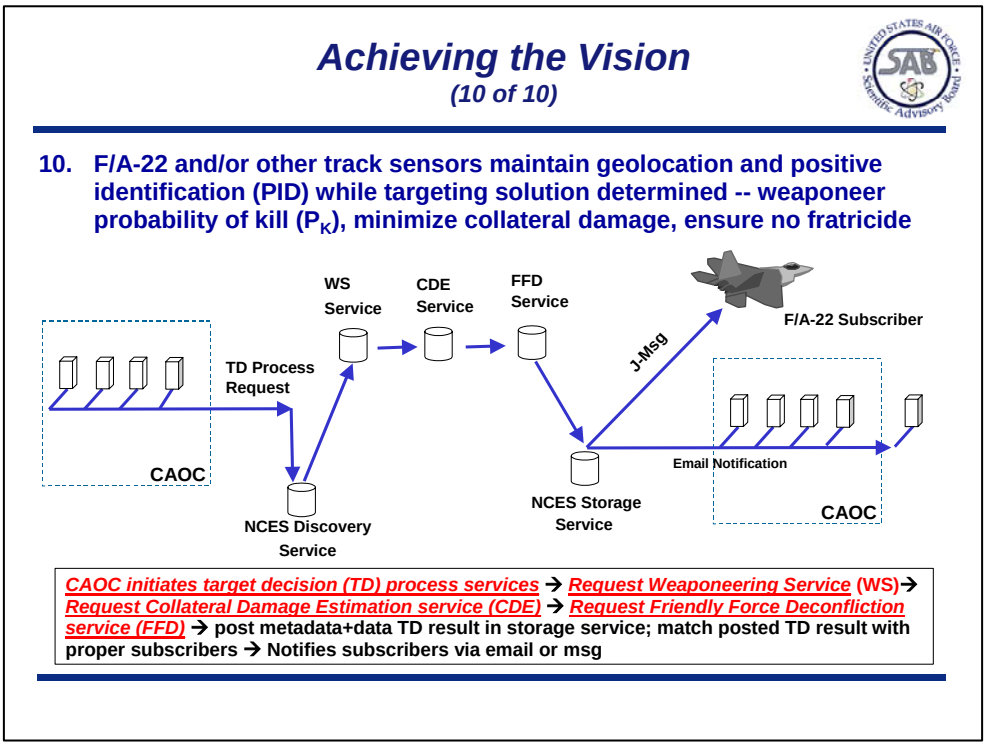
Step 7. The F/A-22 is now subscribed to any targeting decision messages aligned with its mission. The users in the CAOC utilize the NCES collaboration service to establish a session via collaboration services such as whiteboard and chat. Other appropriate CAOC users are invited to attend the session during which the group reaches a targeting decision. The targeting decision is ready to be published as a message to the airborne F/A-22. The collaborative service discovers the messaging service and publishes a targeting decision message to the messaging service. The messaging service matches the incoming message with all appropriate subscribers. In this case the subscribing F/A-22 matches the criteria for the targeting message, and the targeting message is sent via Link-16 to the aircraft.



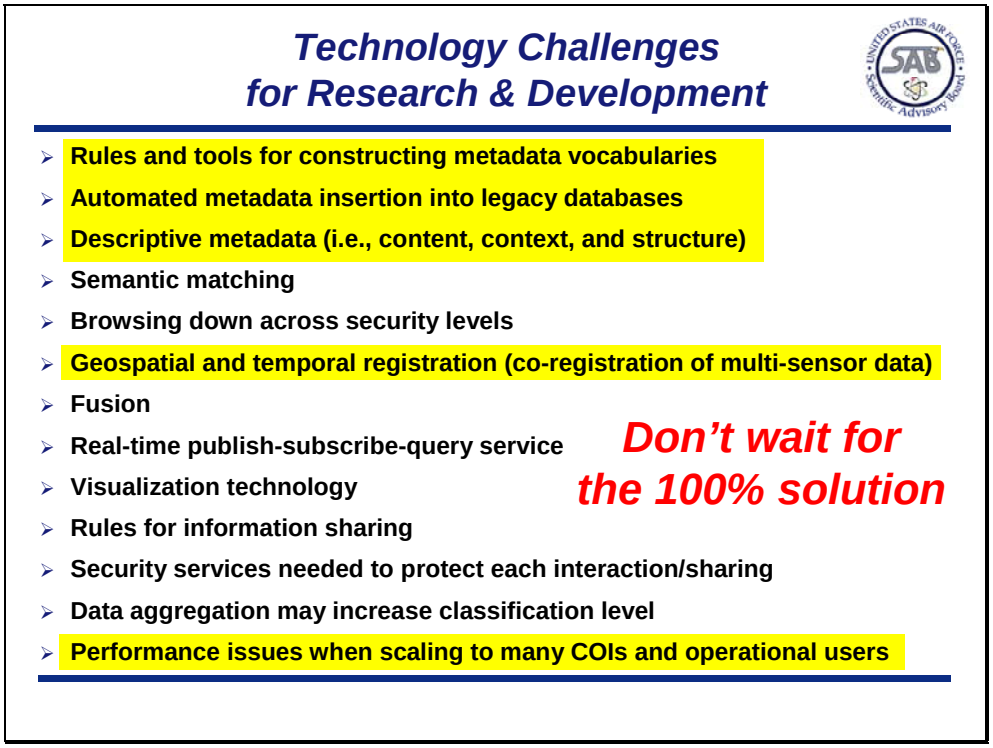
Step 8. The target is engaged by the F/A-22 with the weapon determined by the targeting solution. The F/A-22's sensors collect and post XML-marked up sensor data to the storage service and notifies all subscribing CAOC users of the existence of new relevant F/A-22 sensor data via an email message through the Portal.



Step 9. The CAOC initiates via the portal a request for Weapons Effects Assessment (WEA) utilizing the new sensor data collected by the F/A-22. The NCES IA/Security service authenticates the CAOC user and then passes the request onto the Discovery service to lookup and locate the WEA service somewhere in the GIG. The WEA is located, and the service request is initiated. The WEA gathers the relevant data from the NCES storage service and computes the WEA. The WEA result notification is posted to the Messaging service that sends a notification email to all subscribing CAOC users who can access the WEA result through the portal and determine if a re-strike is required.



Step 10. The F/A-22 remains on station while the WEA is computed and a re-strike decision is determined. A re-strike decision is reached and approved. As a result, the targeting solution process is initiated. The CAOC users initiate requests to the Weaponeering Service (WS), Collateral Damage Estimation (CDE) service, and Friendly Force Deconfliction (FFD) service that result in a targeting solution for a re-strike. These services are requested in order to ensure a proper targeting solution is reached. The CAOC user is authenticated by the IA/Security service. The service requests are sent in order to the Discovery service that locates each service in the GIG and orchestrates the sequence of service initiation. The services are initiated in sequence with the result of one passed to another until the Friendly Force Deconfliction service is finished computing. The new targeting solution is posted to the NCES Storage service. Also, the Message service is initiated to send an email message to the proper subscribing CAOC users that a new targeting solution has been reached and is posted for review.



While the SOA is a good choice, the current off-the-shelf technology is not adequate for all steps. The Commercial sector does not have the same combination of challenges as the Air Force. Therefore, it is not expected that commercial solutions satisfy all of these technology shortfalls. A number of technology challenges call for continued research and development.

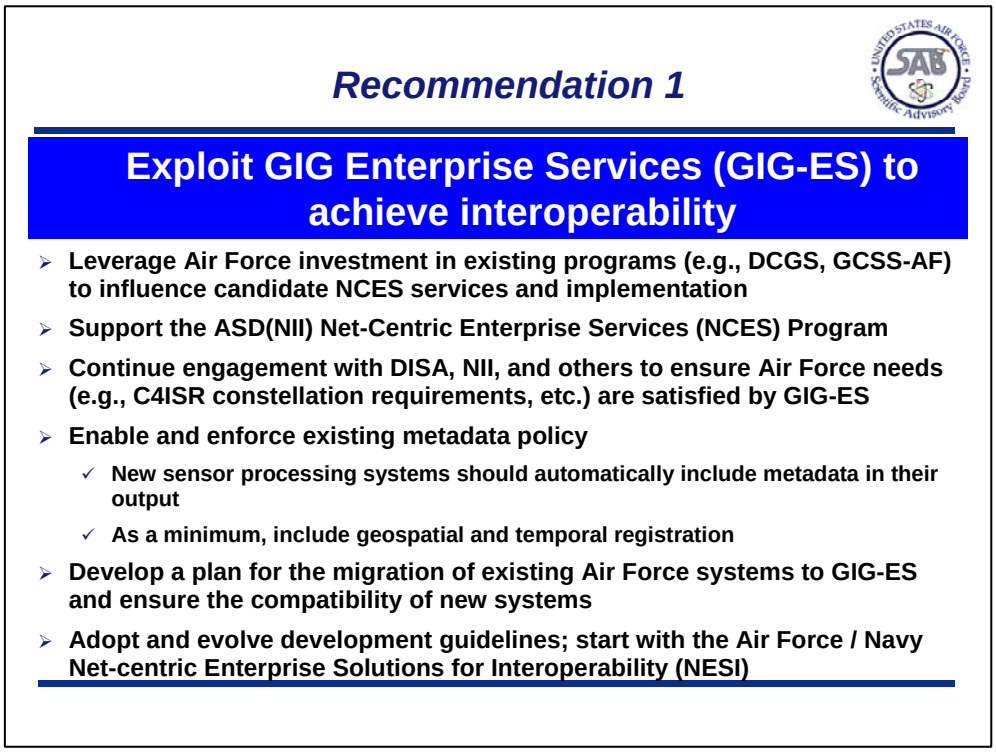
Metadata and common vocabularies: Associating metadata with each data resource and establishing common mission-related vocabularies are required for correct understanding of that metadata. This is an essential part of information discovery, machine-to-machine interoperation, pedigree, and access control. Technology shortfalls include methodology and tools for producing these vocabularies and methods of attaching metadata to legacy resources without extensive manual intervention.

Performance and survivability: The Enterprise Service Bus (ESB) distributes information via a content-based publish/subscribe/query service. Performance requirements with sensor data pose unmet technical challenges, such as large volume and velocity of data as well as many consumers needing a (variable) small fraction of the available data. Quality of service requests from many consumers must be combined and prioritized according to the commander's policy choices. The ESB infrastructure must be distributed and must continue to perform as infrastructure nodes unpredictably enter and leave the network.

Information assurance: The security services ensure proper authorization before participants are able to utilize and post information. Access decisions will be authorized by rules that evaluate the metadata attributes of the data resource in question. For reasons of flexibility, the metadata attributes used in access control should not reflect the results of an access decision. Instead, the access rules should examine the metadata attributes that form the basis of the decision. In this way, access policy can be changed without having to re-label all of the affected

information objects. This concept is called Metadata-Derived Releasability (2004 NECO study). While the implementing technology is available, more work is needed to show it can be dependably applied and used as the basis for revised rules concerning security accreditation and certification.

COI and domain services: There are technology challenges associated with services that consume and exploit information provided through the SOA. Fusion and visualization are well known problems that will endure. A geospatial-temporal registration service is a pressing need that could be implemented quickly, to great advantage.



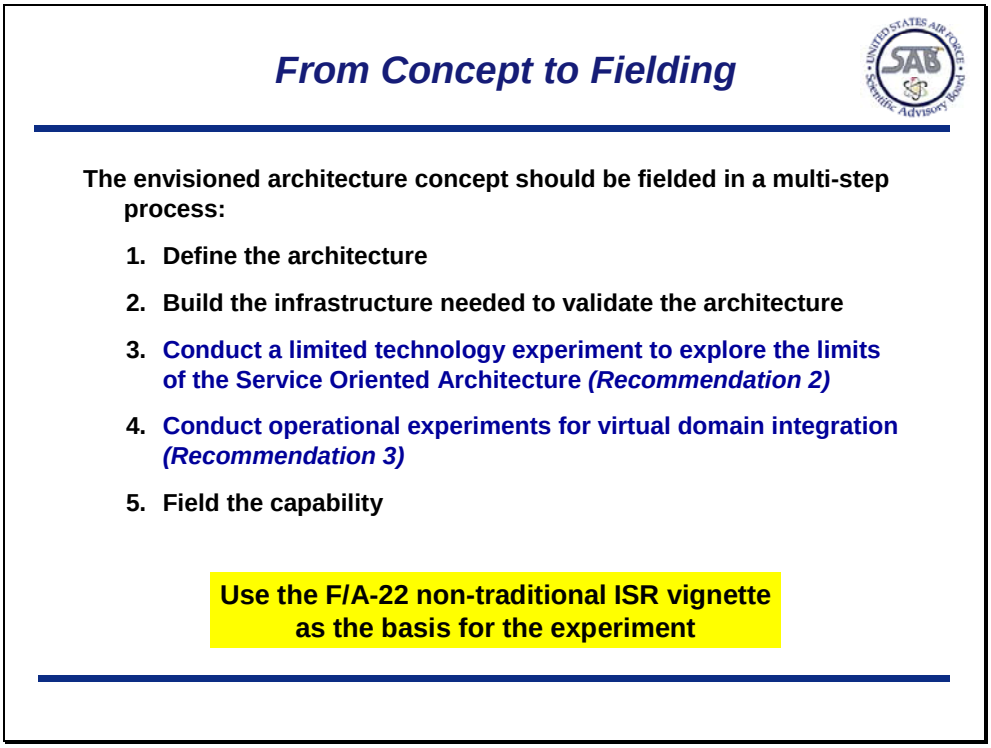
NCES is a new program intended to develop the core infrastructure services for the GIG. The success of this program is important to the Air Force – it needs to be built and built right! There are four things the Air Force can do today to make this success more likely:

1. Identify the requirements of developing and future AF programs, and make sure these are included in the NCES requirements. Also, help NCES think through how these systems will be operated and maintained. For example, the "directory service" needs to supply information about people in the Air Force. That information needs to be created and maintained in a decentralized manner.

2. Several important, existing AF programs are building core infrastructure services for internal use. The experience gained should be transferred to the NCES program. The contributed value may be in the design of the service interfaces, experience with commercial standards, or specific implementation choices. Lessons learned about service administration and maintenance are also important.

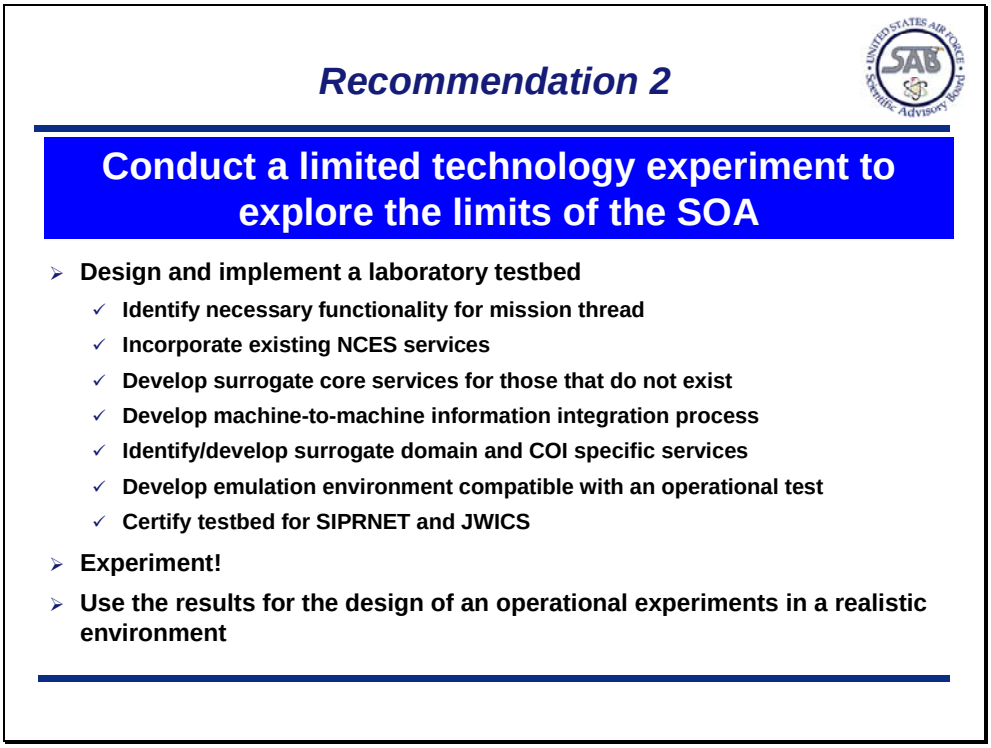
3. AF programs should not be discontinued while the NCES services are being developed. They must, instead, consider the necessary changes in their infrastructure capability now, so that they can interoperate with the NCES infrastructure later. The time to plan for this change is now.

4. NESI contains useful knowledge about what programs can do today to make their systems interoperate using the loose-coupled approach promoted by this study. NESI is not a complete set of guidelines, but it is a useful starting point.



The application of the Service Oriented Architecture (SOA) approach to domain interoperation begins by identifying key structural elements of the four architectural layers (e.g., mission, COIs, domains, and infrastructure). Using the F/A-22 non-traditional ISR vignette as the mission thread for the experiment, appropriate COI's are identified and included as part of the architectural structure. For example, the mission thread must include appropriate information elements from the intelligence, surveillance, and reconnaissance communities, whether traditional or non-traditional. In defining the mission information, the information required by decision-makers, from commander to operator, must be identified. In turn, the domains are determined (e.g., the aircraft platform, NSA, NGA, CAOC, and etc.) that constitute the sources and users of the information needed to execute the mission thread. Having structured the mission, COI, and domain layers, the services that are instrumental in the mission execution processes can be defined. Principles upon which the infrastructure architecture is defined must enable the interoperable system to respond to unexpected events.

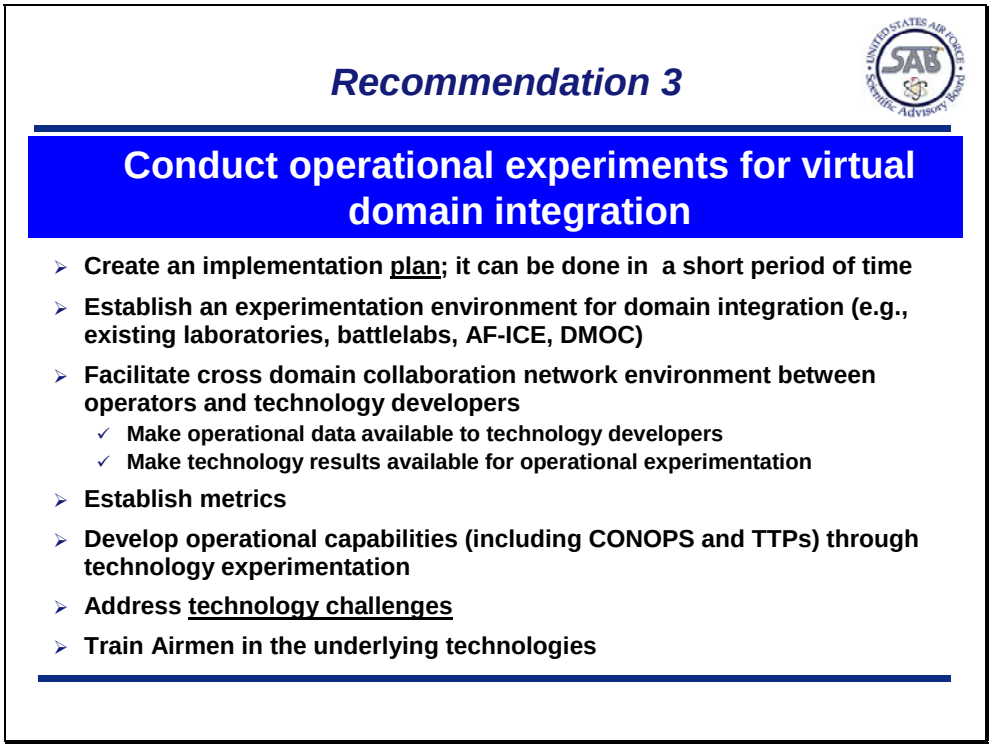
The technology experiment must produce a capability that responds to the mission needs that are established from the assessments conducted during the definition of the architecture. When a useful capability has been demonstrated, experimentation in an operational environment should provide a realistic look at the behaviors that are promised. Successful completion of the operational experiment should then move quickly to fielding of the new capabilities. Problems that are uncovered can be returned with useful insights to the next spiral of the technical experimentation.



The most efficient and timely method for developing fieldable, capability-based products on an SOA is via a sustained series of experiments, with the best ideas leading quickly to operational demonstration and use. As a first step toward fielding, a limited technology experiment should be conducted in a laboratory testbed environment. Since the NCES core services are not yet fully delivered, the testbed should incorporate the available services and develop/procure surrogates for the missing services. Some care should be applied to make the testbed evolve naturally to the NCES core services, as they are made available. In addition, the testbed environment should include simulations of the machine-to-machine connection and integration processes with range and fidelity sufficient to accommodate realistic mission threads.

The specific mission threads identified for experimentation should be analyzed to identify the domain and COI specific services that are needed to accomplish each mission thread. Depending on the specific mission thread, many of the specific services likely exist or can be adapted from existing products; the balance should be developed.

It is likely that one of the "long poles" for the system will be the certification of the system to attach to Joint Worldwide Intelligence Communications System (JWICS) and the SECRET Internet Protocol Router Network (SIPRNET). These network attachments will be critical to acquiring operational data for the use of the development team and for the operation of the testbed. Certification should be pursued as quickly as possible.

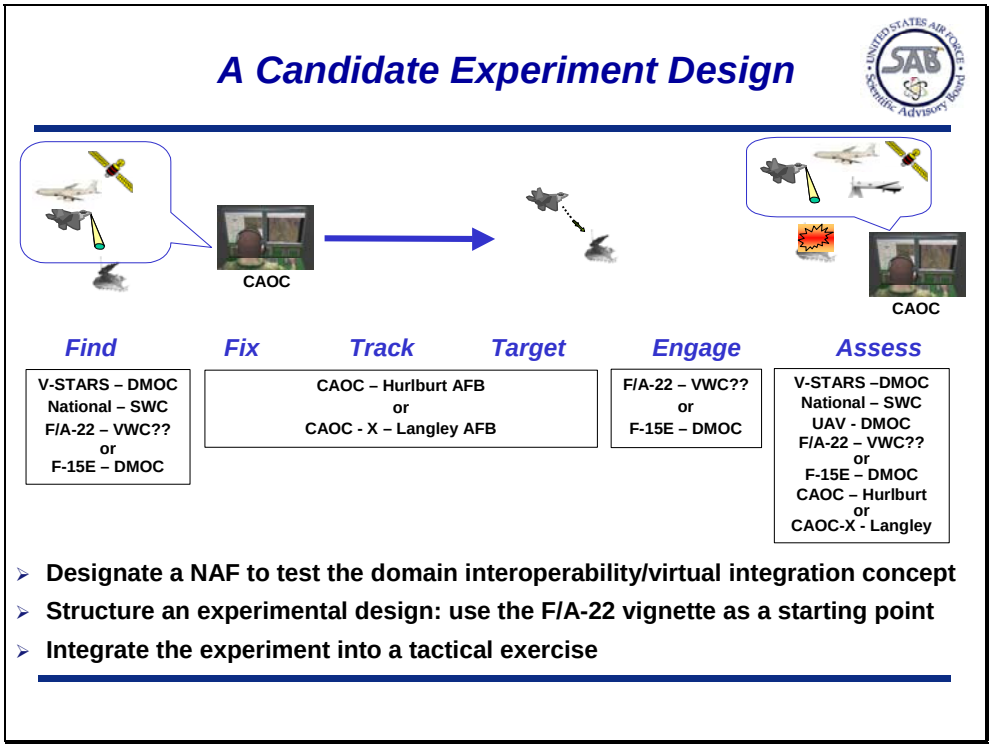


An operational experiment is critical to validating the architecture and technical concepts. Moreover, it provides the opportunity for operational personnel to experiment with the capabilities, to provide valuable feedback to the technical team, and to devise CONOPS and TTPs for the eventual fielding of the capability.

The Air Force Distributed Mission Operations (DMO) infrastructure (hardware, software, networking, and personnel) is ideal for operational experimentation, though it has been heretofore a training and operations capability in frequent use by air operations personnel. However, not all elements of the DMO are used in each training event. Furthermore, the Air Force has been developing the Air Force Integrated Collaborative Environment (AF-ICE). Both environments include capabilities that can be used to the Air Force's advantage and, when available, to conduct the recommended experimentation. The instantiation of the SOA in a virtual combat environment is complex, and, hence, careful planning is required.

A net-centric approach, which connects the researchers and technology developers to the operators along with the use of experimentation environments, will enable timely incremental fielding of capability. Following this recommendation will expose the development community to the current issues being faced by the operators via access to operations data and, conversely, will allow operators to discover emerging technical capability that may apply to the current situation. Since the net-centric architecture and technology represent a departure from past Air Force practices, training of the Airmen who act as information producers, managers, and consumers in the fundamental precepts of the proposed approach is a vital part of the undertaking.

This Study recommends the pilot project implementation plan be developed within 90 days and be constructed collaboratively with technologists and operators in a small team.



As a thought experiment, consider a first cut at an operational experiment of the nature envisioned here.

Available components may be brought together under the leadership of a Numbered Air Force (9th AF, for example) for testing based on an experimental design jointly structured by technical and operational personnel. A Flag exercise will ensure that resources are efficiently assimilated and that a realistic script is incorporated.

Under our concept, elements that address the F/A-22 (or similar) vignette are brought together in an exercise to define an experimental design. The experiment should then be moved to a tactical exercise for a full evaluation.

As success is achieved, a plan for incremental fielding may be devised.

Summary

- **Affirm the goal of interoperability:**
  - ✓ **Focus on *information integration (virtual domain integration)***
  - ✓ **Continue *monolithic systems integration only* where essential**
- **Start with critical mass, but small; build incrementally**
- **The Way Ahead**
  - ✓ **Adopt a Service Oriented Architecture (SOA)**
  - ✓ **Accelerate metadata tagging program (structure, rules, tags)**
  - ✓ **Train Airmen in the underlying technologies**
  - ✓ **Experiment to match technology options with operational needs**

Interoperability is an achievable goal that should be approached principally through data integration, as contrasted with system integration. There will be cases where system integration will be necessary to achieve a specific objective. (Performance, safety, and security are three such potential justifications.)

To achieve this goal, it is possible to start small and build incrementally, but it is very important to start with at least a critical mass (enough to get the process started and keep it running). Successful information integration efforts depend critically on elimination of barriers to information sharing across the enterprise.

The criticality of metadata tagging cannot be over-emphasized. It is the metadata that enables the discovery process and the higher-level fusion processes.

Appendix A: Terms of Reference

USAF SCIENTIFIC ADVISORY BOARD 2005 AD HOC STUDY

Domain Integration

Terms of Reference

BACKGROUND

Warfighters incur significant delays when humans are manually manipulating data to provide integration or cognitively integrating multiple sources of data. The ability to horizontally integrate multi-INT information from space, air, and ground at a machine-to-machine level will enable the Air Force to rapidly and seamlessly integrate ISR with Command and Control systems to address time sensitive targets. The 2003 SAB study on Machine-to-Machine integration postulated a construct in which different domains (e.g., SIGINT, IMINT, MASINT), each with its own internal "domain architecture", became components of a common information architecture to enable information sharing without paying the cost of full pair-wise integration of the component systems. The 2004 SAB study on Network Enabled Coalition Operations (NECO) proposed a high-level information architecture for addressing CAOC needs at the operational level. The next step is the detailed definition of this architecture that enables rapid domain integration and is conformant to the NECO requirements.

STUDY PRODUCTS

Briefing to SAF/OS & AF/CC in October 2005. Publish report in December 2005.

CHARTER

The study should address the following issues and others it uncovers in the process, and provide appropriate recommendations:

Consider, as a basis, the findings and recommendations of the SAB 2003 Summer Study, "Technology for Machine-to-Machine Intelligence, Surveillance, and Reconnaissance Integration" and the requirements identified in the SAB 2004 study on Network Enabled Coalition Operations.

Review commercial information architecture models that address similar needs and solutions for domain integration.

Suggest the elements of an architecture that enables rapid and seamless domain integration.

Consider elements of the solution that address DOD and Air Force information assurance (IA) requirements, including the integration of non-DOD and coalition partners.

Identify specific areas in which the Air Force needs to focus basic and applied research in information technology and networking to adapt (and adapt to) the commercial marketplace.

(This page intentionally left blank.)

Appendix B: Study Members

Study Leadership
Dr. Alexander Levis, Co-Chair
Dr. Peter Worch, Co-Chair

Study Panel
Dr. Wanda Austin
Ms. Monica Chandochin
Dr. "Doc" Dougherty
Mr. Rich Haas
Dr. Mark Linderman
Mr. Jaan Loger
Mr. Rick Metzger
Dr. Scott Renner
Mr. Thomas "Skip" Saunders
Mr. Howard Schue
Dr. Hal Sorenson
Dr. Grant Stokes

General Officer Participant
Maj Gen Robert Elder, Vice Commander, Air University

Study Management
Maj Kyle Gresham, USAF – Project Manager
Maj Jennifer Krischer, USAF – Executive Officer
Maj Robert Renfro, USAF – Technical Writer

(This page intentionally left blank.)

Appendix C: Acronyms and Abbreviations

AF	Air Force
AF SAB	Air Force Scientific Advisory Board
AF-ICE	Air Force Integrated Collaborative Environment
AF/XI	Deputy Chief of Staff for Warfighting Integration (now SAF/XC)
AFC2ISRC	Air Force Command, Control, Intelligence, Surveillance, and Reconnaissance Center
AFRL/IF	Air Force Research Laboratory, Information Directorate
AOC	Air Operations Center
ASD(NII)/DOD CIO	Assistant Secretary of Defense for Networks and Information Integration / Chief Information Officer
ATO	Air Tasking Order
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CAOC	Combined Air Operations Center
CAOC-X	Combined Air Operations Center – Experimental
CDD	Capabilities Development Document
CDE	Collateral Damage Estimate
CFACC	Combined Forces Air Component Commander
COC	Coalition Operations Center
COI	Communities of Interest
CONOPS	Concept of Operations
CoT	Cursor on Target
CSAF	Chief of Staff of the Air Force
DAA	Designated Accreditation Authority
DARPA	Defense Advanced Research Projects Agency
DCFACC	Deputy Combined Forces Air Component Commander
DIB	Distributed Common Ground Systems Integrated Backbone
DISA	Defense Information Systems Agency
DOD	Department of Defense
DCGS	Distributed Common Ground Systems
DMO	Distributed Mission Operations
DMOC	Distributed Mission Operations Center

ESB	Enterprise Service Bus
ESC/EN	Electronic Systems Center, Engineering Directorate
EITS	Enterprise Information Technology Services
FCS	Future Combat System
FFD	Friendly Force Deconfliction
FS	Fusion Service
Geoloc	Geolocation
GCSS	Global Combat Support System
GIG	Global Information Grid
GIG-ES	GIG Enterprise Services
GO	General Officer
GS	Geolocation Service
GT	Geospatial and Temporal
GTR	Geospatial and Temporal Registration
HUMINT	Human Intelligence
JWICS	Joint Worldwide Intelligence Communications System
IA	Information Assurance
ID	Identification / Identification Service
IMINT	Imagery Intelligence
INT	Intelligence
ISR	Intelligence, Surveillance, and Reconnaissance
IT	Information Technology
J-MSG	J-Series Message (Link 16)
JFCOM	United States Joint Forces Command
M&S	Modeling and Simulation
MAJCOMS	Major Commands
MASINT	Measurement and Signature Intelligence
Msg	Message
MTM	Machine-to-Machine
Multi-INT	Multi-Intelligence
NAF	Numbered Air Force
NASIC	National Air and Space Intelligence Center
NATO	North Atlantic Treaty Organization

NCOIC	Network Centric Operations Industry Consortium
NECO	Networking to Enable Coalition Operations (2004 SAB study)
NESI	Net-Centric Enterprise Solutions for Interoperability
NCES	Net-Centric Enterprise Services
NGA	National Geospatial-Intelligence Agency
NRO	National Reconnaissance Office
NRO/DDSE	Deputy Director for System Engineering, National Reconnaissance Office
NSA	National Security Agency
NSSO	National Security Space Office
NTISR	Non-Traditional Intelligence, Surveillance, and Reconnaissance
OEF	Operation Enduring Freedom
OIF	Operation Iraqi Freedom
OSD	Office of the Secretary of Defense
P_k	Probability of Kill
PID	Positive Identification
QoS	Quality of Service
R&D	Research and development
RAAR	Responsibility, Authority, Accountability, and Resources
ROE	Rules of Engagement
SAB	(Air Force) Scientific Advisory Board
SAF/AQ	Assistant Secretary of the Air Force (Acquisition)
SAF/XC	Chief of Warfighting Integration and Chief Information Officer for the Office of the Secretary of the Air Force
SecAF	Secretary of the Air Force
SIAP	Single Integrated Air Picture
SIGINT	Signals Intelligence
SIPERNET	SECRET Internet Protocol Router Network
SOA	Service Oriented Architecture
SOF	Special Operations Forces
SOSCE	System-of-Systems Common Operating Environment
STRATCOM	U.S. Strategic Command
SWC	Space Warfare Center
TD	Target Decision

TOR	Terms of Reference
TST	Time Sensitive Targets
TTPs	Tactics, Techniques, and Procedures
UAV	Unmanned Aerial Vehicle
UD	Update / Update Service
URL	Uniform Resource Locators
USAF	United State Air Force
USCENTAF	U.S. Central Command Air Forces
USCENTCOM	U.S. Central Command
UsecAF	Under Secretary of the Air Force
VWC	Virtual Warfare Center
WEA	Weapons Effects Assessment
WS	Weaponeering Service
XML	Extensible Markup Language

Appendix D: Organizations Visited

Air Force
Chief of Staff of the Air Force
Under Secretary of the Air Force
Deputy Chief of Staff for Warfighting Integration, Headquarters U.S. Air Force
Air Force Command, Control, Intelligence, Surveillance, and Reconnaissance Center
Air Force Electronic Systems Center
Air Force Distributed Mission Operations Center
National Air and Space Intelligence Center (NASIC)
Air Force Research Laboratory

Department of Defense
Assistant Secretary of Defense for Networks and Information Integration
National Security Space Office (NSSO)
Defense Information Systems Agency (DISA)
National Reconnaissance Office (NRO)
Defense Advanced Research Projects Agency (DARPA)
US Joint Forces Command
US Strategic Command
Joint Single Integrated Air Picture Systems Engineering Organization (JSSEO)
Deputy Assistant Secretary for Research and Technology, Chief Scientist, Army
Future Combat System, System of System Common Operating Environment

Industry
BAE Systems
The Boeing Company
International Business Machine
Lockheed Martin Corporation
Network Centric Operations Industry Consortium
Northrop Grumman Corporation

(This page intentionally left blank.)

Appendix E: Distribution

Air Force Leadership
Secretary of the Air Force
Chief of Staff of the Air Force
Under Secretary of the Air Force
Vice Chief of Staff of the Air Force

Air Force Secretariat
Assistant Secretary of the Air Force for Acquisition
- Deputy Assistant Secretary of the Air Force for Science, Technology, and Engineering

Chief of Warfighting Integration and Chief Information Officer, Office of the Secretary of the Air Force

Air Staff
Assistant Vice Chief of Staff of the Air Force
Deputy Chief of Staff of the Air Force for Air and Space Operations
Deputy Chief of Staff of the Air Force for Plans and Programs
Deputy Chief of Staff of the Air Force for Test and Evaluation
Director of the Air National Guard
Chief of Air Force Reserve
Chief Scientist of the Air Force
Scientific Advisory Board Military Director

Air Force Major Commands
Air Combat Command
- ACC Chief Scientist

Air Education & Training Command
Air Force Materiel Command
- Requirements Directorate

Air Force Reserve Command
Air Force Space Command
- Space Warfare Center

Air Force Special Ops Command
Air Mobility Command
Pacific Air Forces
U.S. Air Forces in Europe

Other Air Force Elements
Aeronautical Systems Center
Air Force Command, Control, Intelligence, Surveillance, and Reconnaissance Center
Air Force Distributed Mission Operations Center
Air Force Electronic Systems Center
Air Force Institute of Technology
- Center for Systems Engineering

Other Air Force Elements continued
Air Force Research Laboratory
Air Warfare Center
National Air and Space Intelligence Center
Space and Missile Systems Center

Office of the Secretary of Defense
Under Secretary of Defense for Acquisition, Technology, and Logistics
- Director of Defense Research and Engineering

Assistant Secretary of Defense for Networks and Information Integration
Office of Program Analysis and Evaluation, Cost Analysis Improvement Group

Joint Chiefs of Staff
Joint Chiefs of Staff, Director of C4 Systems
Joint Chiefs of Staff, Director of Operational Plans and Interoperability
Joint Single Integrated Air Picture Systems Engineering Organization

Unified Commands
U.S. Joint Forces Command
U.S. Strategic Command

Defense Agencies
Defense Advanced Research Projects Agency
Defense Information Systems Agency
Missile Defense Agency
National Reconnaissance Office
National Security Space Office

U.S. Army
Deputy Assistant Secretary for Research and Technology, Chief Scientist
Future Combat System, System of System Common Operating Environment

Advisory Boards
Army Science Board
Defense Policy Board
Defense Science Board
Naval Research and Advisory Committee
Naval Studies Board

Industry
BAE Systems
The Boeing Company
International Business Machine
Lockheed Martin Corporation
Network Centric Operations Industry Consortium
Northrop Grumman Corporation

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and manipulating the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY (*Leave Blank*)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	July 2005	Final, January 2005 – July 2005

4. TITLE AND SUBTITLE
Domain Integration: Executive Summary and Annotated Brief

5. FUNDING NUMBERS

6. AUTHOR(S)
Prof. Alexander Levis, Dr. Peter Worch, Maj Gen Robert Elder, Dr. Wanda Austin, Ms. Monica Chandochin, Dr. "Doc" Dougherty, Mr. Thurman Haas, Dr. Mark Linderman, Mr. Jaan Loger, Mr. Rick Metzger, Dr. Scott Renner, Mr Thomas "Skip" Saunders, Mr Howard Schue, Dr. Hal Sorenson, Dr. Grant Stokes

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
HQ USAF/SB
1180 AF PENTAGON RM 5D982
WASHINGTON, DC 20330-1180

8. PERFORMING ORGANIZATION REPORT NUMBER
SAB-TR-05-03

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
SAF/OS, AF/CC
AIR FORCE PENTAGON
WASHINGTON, DC 20330-1670

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Public Release

12b. DISTRIBUTION CODE
Distribution A

ABSTRACT (Maximum 200 Words)

The Domain Integration ad hoc study addresses the effective manipulation and transfer of information among warfighters by predominantly machine-to-machine means. More specifically, the vision derived from the Terms of Reference is: The ability to horizontally integrate multi-INT information from space, air and ground at a machine-to-machine level will enable the Air Force to rapidly and accurately integrate data and information across domains to address time sensitive targets. The study team reviewed the current capabilities and technologies, identified an architectural approach, determined the needed technology advancements, and recommends a path through experimentation to fielding.

Interoperability is an achievable goal that should be approached principally through data integration, as contrasted with system integration. We recognize that there will be cases where system integration will be necessary to achieve a specific objective (performance, safety, and security are three such potential justifications). To achieve this goal it is possible to start small and build incrementally, but it is very important to start with at least a critical mass (enough to get the process started and keep it running). Successful information integration efforts depend critically on elimination of barriers to information sharing across the enterprise.

14. SUBJECT TERMS
Domain Integration, Domain, Integration, Interoperability, interoperation, machine-to-machine, integrate, system of systems, architecture, metadata, Communities of Interest, COI, Service Oriented Architecture, SOA, stovepipe, net-centric, Global Information Grid, GIG, GIG Enterprise Services, GIG-ES, Net-Centric Enterprise Services, NCES, Distributed Mission Operations, DMO, experiment, experimentation, F/A-22, USAF, Air Force, Scientific Advisory Board, SAB

15. NUMBER OF PAGES
70

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASS	UNCLASS	UNCLASS	Public Release

(This Page Intentionally Left Blank.)