Command and Control

Peter M. Trask, Frederic T. Case, Steven L. Forsythe, Thomas M. McNamara Jr., Paul D. North, Kim E. Richeson, Christine O. Salamacha, and John J. Tamer

The Global Engagement Department (GED) is addressing critical challenges in command and control (C2) for the DoD and other government agencies by providing capabilities for seamless information sharing, collaboration, and decision making across national, strategic, operational, and tactical echelons of command. These capabilities include methodologies and tools to dynamically assemble and enable virtual teams of warfighters and subject-matter experts to improve responses to military or homeland security crises, as well as the capability to evaluate and assess warfighter value, robustness, and interoperability of proposed C2 implementations by using a broad range of measurements. These capabilities are based on a net-centric data strategy and service-oriented architecture and are built on the Global Information Grid. This article provides some examples of GED work in these areas.

INTRODUCTION

The importance of information sharing and rapid decision making has increased dramatically in the new national security environment. There is no more compelling example than the events leading up to the 9/11 attacks on our homeland where decision makers were hampered by inconsistent situational understanding and lack of effective collaboration across all command levels.[1]

The goal of the Global Engagement Department (GED) is to achieve seamless command and control (C2) for decision makers at all echelons of command (national, strategic, operational, and tactical) by providing unprecedented access to real-time actionable information and comprehensive battlespace understanding. Through effective distributed collaboration, we can achieve (*i*) a more complete and current under-

standing of the situation; (*ii*) faster, accurate, efficient planning; (*iii*) better, timely, efficient decision making; and (*iv*) adaptable execution. We believe that this will allow our forces to shorten the kill chain and to achieve desired effects on demand in time-sensitive situations.

Our approach is to leverage the DoD's Global Information Grid (GIG) and net-centric implementation strategy, where data and information are made visible, accessible, and understandable to all forces with appropriate clearances. By using an enterprise-wide service-oriented architecture, relevant, timely, and accurate information will be available to decision-makers at all levels throughout all phases of planning and execution. Information will be correlated, aggregated, and displayed in formats that meet the warfighters' needs—in user-defined operating pictures (UDOPs).

Commanders at all levels will have consistent situational information leading to a shared understanding of the battlespace and will be able to collaborate effectively using the GIG as a virtual collaborative table, as depicted in Fig. 1.

Enabling effective collaboration is a principal GED C2 thrust area. Our collaboration work is not just about the tools (e.g., white-boarding, chat), but rather about establishing an environment, including people, data, workspaces, processes, and tools, that can be established rapidly and dynamically for a particular time-critical mission.

We are developing a C2 evaluation capability to measure the value of current and proposed C2 applications and services and to measure the extent to which the GIG with bandwidth limitations, latencies, or other impairments affects the performance of C2 applications. This C2 evaluation capability is viewed as critical to establishing a role in C2 that APL traditionally serves in several areas—that of trusted agent, assisting government sponsors in determining whether an industry solution satisfies a stated need and adds value to the warfighter.

We have established a capability to measure and assess the performance of C2 processes in an operations center. This capability is important because it provides

Figure 1. This virtual collaborative "table" uses the GIG as a foundation and establishes a distributed environment for decision makers at all echelons of C2.

feedback to operators on their performance after an exercise or training event. It also can be used to measure the warfighting value of proposed technology or process improvements. This capability has been introduced into U.S. Air Force (USAF) Combined Air Operations Centers (CAOCs).

Performing analyses and assessments is an important first step before making changes to critical national security capabilities. APL conducted an analysis of how best to transition the existing nuclear C2 (NC2) system to a New Triad C2 system. The results of this analysis are likely to have a significant impact on the future of the New Triad C2 system, and, as a result, on the safety and security of the nation.

In response to the events of 9/11, Congress directed the establishment of an Information-Sharing Environment (ISE) to improve and facilitate sharing of terrorism information. It will provide mechanisms to permit partner agencies at the federal, state, and local levels (e.g., fusion centers) to share data based on common standards. In support of this effort, APL developed an ISE Enterprise Architecture Framework (ISE EAF) to guide the implementation of the ISE. This EAF will provide mechanisms to permit governmental agencies to share data rapidly in response to future crises.

The remainder of the article focuses on a few of GED's C2 programs and initiatives in these areas.

COLLABORATION

The global challenges faced by our nation and our armed forces demand a higher level of agility, seamless access to data, dynamic collaboration, flexibility, interoperability, and interdependence than ever before. The DoD is leveraging advances in computation, networking, and information technologies to provide the GIG and the capabilities required to address these challenges. A net-centric environment is considered essential to revolutionizing C2 to yield the leaner, more agile C2. "Agility is increasingly becoming recognized as the most critical characteristic of a transformed force, with network-centricity being understood as the key to achieving agility."[2]

Collaboration is a critical component of C2 today, and the promise of net-centricity is that broader access to data and people as well as new opportunities for collaboration will improve and even transform future C2. Although collaborative and networked approaches to C2 are common within the DoD, the technological capabilities envisioned for the GIG will literally enable anyone to engage anyone else in a decision-making process irrespective of distance, time, organization, and organizational structure. Over the last several years, GED has examined how collaborative C2 could be conducted in a GIG environment. In 2003, an APL team that included GED staff supported Horizontal Fusion, a key DoD net-centric transformation initiative sponsored by the Office of the Assistant Secretary of Defense for Networks and Information Integration. GED's involvement in Horizontal Fusion's Quantum Leap-2 demonstration provided the inspiration for the Dynamic Collaborative Action Team (DCAT) framework developed within GED.

A DCAT is a dynamic and to some degree ad hoc grouping of organizations or personnel activated for a specific mission or operational task irrespective of command. These ad hoc teams also are sometimes called "Communities of Action." When such teams are activated to address unique operational problems, the GIG environment will enable them to discover and utilize new data and include members outside of routine organizational and command structures. The teams will leverage prior knowledge and previously defined structures and also use GIG capabilities that allow them to build membership dynamically and customize tactics, techniques, and procedures (TTPs) for the employment of people, processes, data, and tools. The objective of the DCAT framework developed within GED is to provide a flexible structure to enable dynamic, collaborative, action-oriented teams to operate effectively and exploit the benefits of the GIG to achieve mission success.

As depicted in Fig. 2, the DCAT framework spans the building of patterns that reflect pre-crisis planning and lessons learned from previous operations, activation of a specific team using an existing pattern, collaborative

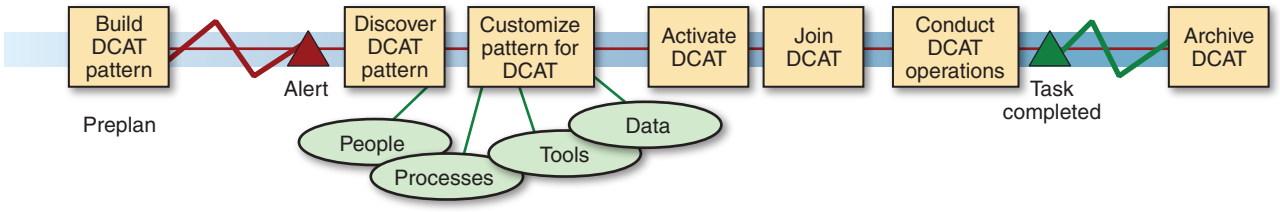

Figure 2. DCAT framework showing the sequence of events involved in establishing a dynamic team in response to a time-critical event.

activities during operations, and, finally, deactivation of the team and archiving of a "new" pattern. The concept of patterns is a key component of the DCAT framework. Patterns provide the initial structure for the team and its workspaces. For example, a pattern is intended to contain mission-based objectives, recommendations for team membership based on functional roles, role responsibilities and permissions, and guidelines (e.g., TTPs). It also provides templates for team workspaces that are equipped with content, such as key documents, product templates, and authoritative data sources. When new workspaces are generated by using these templates, they are automatically provisioned with recommended tools and data services and are equipped with embedded mission workflow. Figure 3 shows a representative team workspace implemented in a portal environment, which functions as a point of access to information distributed on a network. It is envisioned that the DCAT pattern will provide the "80% solution" of component parts needed to establish an actual DCAT for a given mission or operation. Pattern-based workspace content and structure would then be customized to better address the unique operational situation and needs of the team (although some constraints may be implemented to enforce best practices).

DCAT patterns will be developed through advanced planning, training, and exercises. War games and exercises are excellent venues to practice the use and refinement of the DCAT framework. Lessons learned from these activities can be used to modify patterns and improve the library of available DCAT patterns. Variant patterns can be created to better suit the operational needs of a given command. Patterns also will be saved and archived at the conclusion of a team's operations for use by similar teams in the future. This provides future collaborative teams with the benefit of the data and tools used, the best practices used, and the roles adopted by previous teams. The ability to leverage past patterns is a powerful advantage over current collaborative planning, training, and operations. Facilitated improvement also involves capturing lessons learned and tagging these lessons with their underlying DCAT pattern.

Over the course of our work in collaborative C2, collaboration technologies evolved to a state where they now support some of the more advanced features defined for the DCAT framework. However, capabilities to dynamically find individuals with the requisite experience, skills, and command authorization to support team activities were found to be lacking. The GED team partnered with colleagues in the Milton Eisenhower Research Center in an Independent Research and Development (IRAD) effort to address some of the challenges associated with building an effective ad hoc team. Sometimes individuals needed for collaborative sessions are known by name, but many times they are not. Criteria specified in a Request for Support may include, for example, desired occupational specialties,

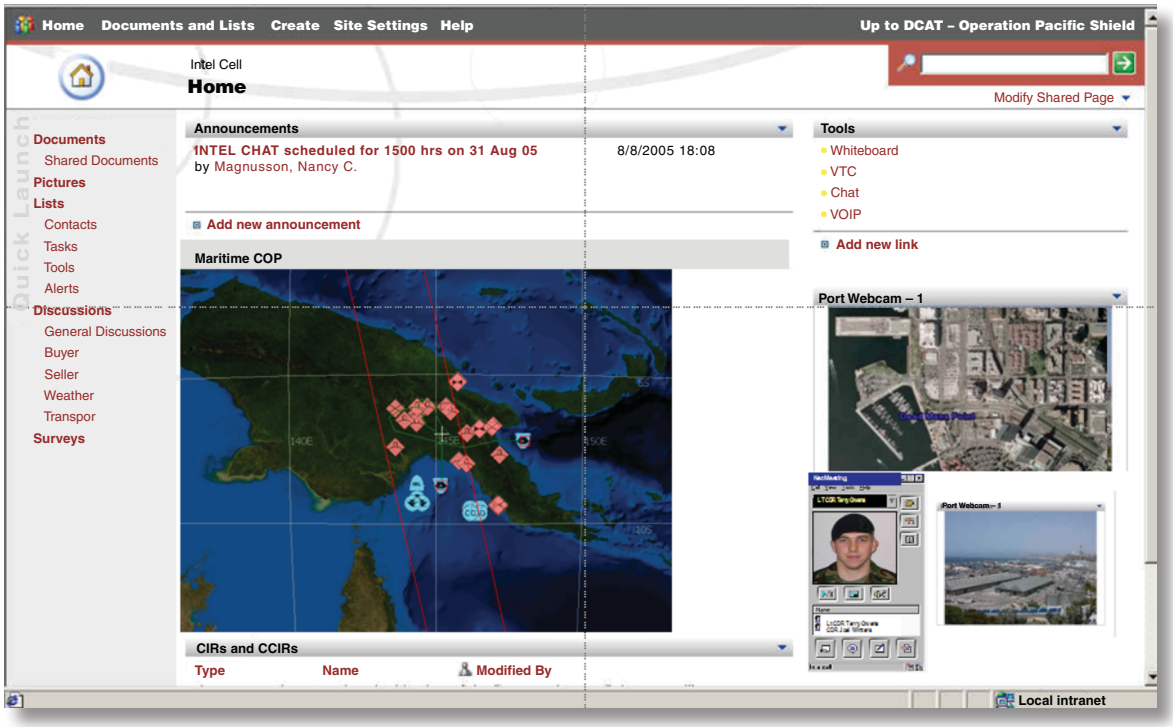

Figure 3. Sample DCAT Intel Cell workspace implemented in a portal environment.

military rank, length of service, organization affiliation, standing operational team membership, previous operational experience and deployments, education, previous training and certification, familiarity with tools, and unique skills. This data are typically stored in a variety of different repositories. The DCAT framework includes the concept of a Virtual Resource Broker that employs knowledge-management technologies to query heterogeneous databases and smart-agent capabilities to semantically interpret and satisfy a DCAT Request for Support. The Resource Broker finds data of interest, correlates data from different sources, and subsequently maps DCAT criteria specified in the Request for Support to individuals.

Work on a prototype DCAT framework started under a number of internal APL investment initiatives. A technical strategy that proved to be successful in implementing the DCAT framework involved exploiting commercial technologies as much as possible and then identifying how these technologies could be extended to provide breakthrough capabilities. Implementation of the framework leveraged web-browser portal technologies and was synchronized with concurrent GED efforts to expose data sources as web services and provide capabilities via a service-based architecture. As previously discussed, work on the Virtual Resource Broker was conducted as collaborative research between GED and the Milton Eisenhower Research Center. The Advanced Geospatial Collaboration Environment (Collabspace) started as a research effort in the former Precision Engagement Department. Although most collaboration environments (chat, instant messaging, etc.) are not geospatially aware, collaboration in the C2 domain typically revolves around three general spaces: geographic location of objects (aircraft, troops, etc.), temporal information (when objects will arrive, depart, etc.), and process information (where users fall in a detailed series of events). Collabspace provided basic text chat and geospatial whiteboarding, allowing users to draw lines, polygons, points, and other objects on the geographic display and share them with other users in a workshop. Advanced text chat capabilities tailored for C2 collaboration included automatic hyperlinking from chat to known geospatial objects and automatic highlighting and capture of directed requests and responses. Multichannel support in a single chat window provided the user with the ability to monitor and converse in multiple chat channels from within the same chat window. Collaboration artifacts such as whiteboard objects were available to web service-enabled C2 systems as an overlay. Subsequent research efforts within GED focused on providing a geospatial visualization capability as a thin client deployed within a portal environment and capable of consuming and producing overlays, providing a geospatial presentation based on semantic content, and extending the DCAT framework to mobile users.

Early APL-funded explorations demonstrated the feasibility of deploying composable C2 capabilities comprising components that are unique to organizations or commands as well as common services that are used enterprise-wide. Encapsulation of mission workflow and business processes into DCAT patterns and workspace design was examined in depth when the DCAT framework was adopted by U.S. Strategic Command (USSTRATCOM) as the underlying framework for the Global Strike Planning (GSP) Global Operations Center–Collaborative Environment (GOC-CE) initiative. GSP GOC-CE was initially called GOC Net-Centric Initiative. The overarching objective of the GSP GOC-CE was to demonstrate a net-centric, globally accessible, user-definable data-sharing and collaboration environment, rapidly created to support a time-sensitive global strike (GS) C2 process. The GOC-CE initiative successfully employed elements of the DCAT framework to create collaborative environments rich with content that could be dynamically generated to address a specific mission. Information was managed through GOC-CE portlets in the collaborative space, providing all users with shared situational awareness. At the same time, each GOC-CE user could adapt his or her personal graphical user interface by adding, deleting, and rearranging portlets (i.e., a UDOP similar to MyYahoo.com). The technical experience gained from GOC-CE, although significant, was eclipsed by the lessons learned compiled from the series of exercises conducted by USSTRATCOM using the GOC-CE environment. Piloting of GOC-CE has provided invaluable insights into how C2 could be conducted in a net-centric environment.

GOC-CE proved to be a compelling exemplar of the DCAT framework. U.S. Joint Forces Command (USJFCOM) was impressed with the capabilities provided by the GOC-CE and decided to adopt a DCAT approach for the Joint Task Force Headquarters (JTF HQ) Turnkey C2 Initiative. Turnkey C2 is an HQ USJFCOM/J8-led cross-directorate project that jump-starts the JTF HQ C2 formation and operations by enabling the JTF Commander and staff to reduce the time it takes to complete their initial mission analysis. This allows the staff to begin working to identify interoperable resource shortfalls within existing service C2 capabilities. The JTF HQ Turnkey Playbook (APL's contribution) prototyped the capability to review and work with established JTF baseline architecture templates before the activation of a new JTF and to assist in jump-starting the formation of new JTFs once a mission is assigned. Before JTF activation, users can examine potential equipment and application shortfalls and identify pre-sourcing solutions and procedures. Pre-mission activities also can include accessing and reviewing reference material, such as training and certification documents, various handbooks, and lessons learned.

Although DCAT-related technical work has proven to be interesting and challenging, we have found that the most difficult challenges to implementing DCAT concepts have to do with cultural resistance and not technology gaps. Such cultural obstacles are to be expected given that DCATs and the DCAT framework represent a transformational C2 concept. The net-centric environment enables DCAT members to fully participate in the development of team products. However, policy, procedures, and culture will need to adapt to address how personnel can be placed within one of these ad hoc teams and be committed to team support at the level required. These individuals will need to be kept apprised of all team objectives, guidance, and procedures without needing physical presence in the team or a designated individual to relay such items. Likewise, personnel systems will need to develop processes to "assign" a person to a team without the need to reassign the individual physically to the team's location. This will include tracking and "crediting" individuals for operational engagement and increased operations tempo when directly supporting military operations without the necessity of deployment to the specific areas of responsibility where the main team effort is focused. Also, personnel systems will need to define individuals' skills and "DCAT readiness" to a degree not currently available today in order to ensure that good matches of possessed skills to needed skills can be made in a more rapid and effective manner than possible with today's deployment support system. Today's reality is that finding and getting the right person for the job in a quick time frame is highly dependent on personal networks, otherwise known as "bubba nets." One of the benefits of a net-centric opportunity is that all warfighters should have equal access to virtual bubba nets that can help them find the right people for their teams. Socializing these and other culture-related aspects of DCAT operations has been one of the objectives of pilot efforts such as GOC-CE and the JTF HQ Turnkey Playbook.

C2 EVALUATION

The DoD has embarked on a path to make force transformation an integral element of national defense strategy. Transformation is a continuing process involving the evolution of concepts, processes, organizations, and technologies. The term "network-centric warfare" is applied to the combination of emerging and evolving TTPs that a networked force can employ to create a warfighting advantage. Network-centric warfare is at the heart of force transformation. Successful transformation hinges on making the right investments in the right area to take full advantage of net-centric warfare and operations technologies and practices.[3]

Net-centric transformation and its associated practice of portfolio management require DoD decision makers to understand how applying net-centric principles to C2 affects operational outcomes. GED's work in C2 evaluation has focused on ways in which modeling and simulation (M&S) techniques can be adapted to provide a foundation for evaluating those effects.

We began this work by establishing a framework, referred to as the Multi-Resolution Modeling Evaluation Framework (MRMEF), to help us evaluate whether the application of net-centric principles to C2 improves the effectiveness and efficiency of C2 in a complex, hybrid architectural environment where net-centric and legacy capabilities and processes co-exist and interoperate. This approach uses scenarios to bound the mission space to be evaluated and employs simulation techniques using multiple levels of fidelity or resolution to evaluate net-centric C2 in that complex hybrid environment. A depiction of the MRMEF is shown in Fig. 4.

The MRMEF contains the entire hardware and software infrastructure needed to support:

- Constructive simulation, which involves a models-only simulation environment
- Virtual simulation, which involves a simulation and test-bed environment with people and hardware/software in-the-loop
- Live simulation, which involves simulation in an exercise environment with real people and real components

Inputs to the framework consist of a set of C2 services or components to be evaluated. These are derived from C2 architectural analysis, C2 gap analysis, C2 requirements definition, etc. A scenario, which is used to define the operational mission (i.e., the problem to be solved), serves as the contextual basis for the evaluation and is used to identify context-specific effectiveness attributes in the form of measures of performance, effectiveness, and force effectiveness. Examples of specific measures at these three effectiveness levels are shown in Fig. 5.

Based on the scenario, chosen from a bounding set of scenarios, and a selected level of modeling fidelity, two simulations are generated, one representing the "as-is" or non-net-centric environment and the other representing the "to-be" environment, which includes net-centric capabilities. The results of executing the two simulations are compared to determine the effects of net-centric capabilities on mission outcomes as represented in the scenario.

A cornerstone to achieving accurate M&S is the ability to understand the underlying C2 processes being represented in the M&S environment. To that end, we have spent a significant amount of time focusing our efforts on C2 process decomposition. An example of

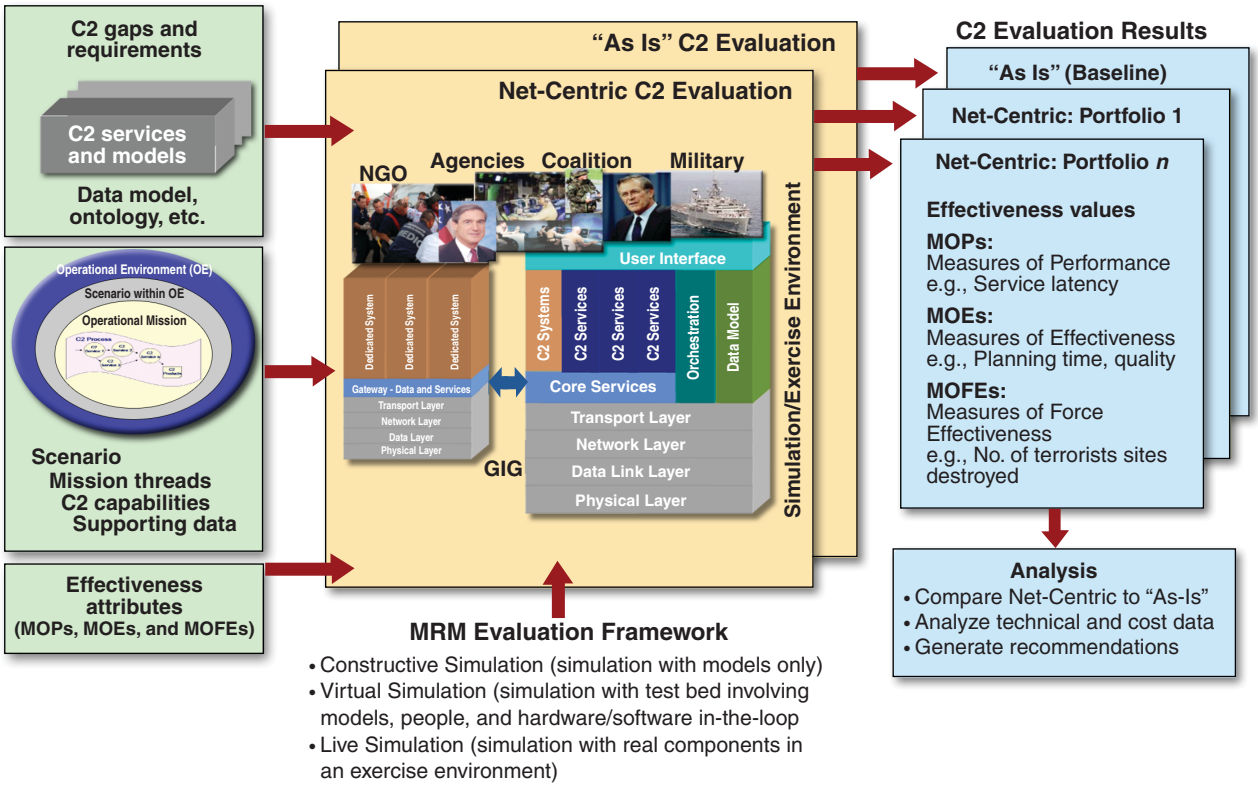

Figure 4. The MRMEF. HW, hardware; NGO, non-governmental organization; SW, software.

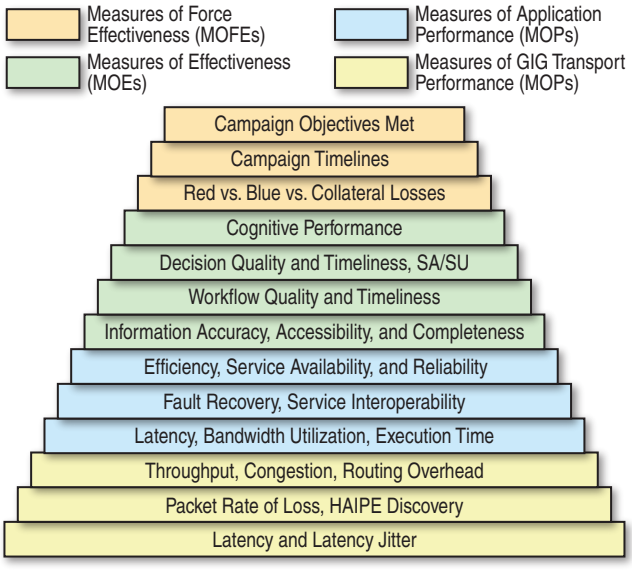

Figure 5. Pyramid of effectiveness attributes. HAIPE, High Assurance Internet Protocol Encryptor; SA, Situational awareness; SU, situational understanding.

that effort is the decomposition of the GS process used at USSTRATCOM. Their GS mission area, as it was characterized in FY05, is decomposed into three high-level elements: adaptive planning, crisis action planning, and execution (Fig. 6).

A further notional decomposition of one of those areas, crisis action planning, shows how low-level process elements could be linked to existing systems and how selected functional portions of those existing systems can be targeted as potential candidates for instantiation as net-centric web services (Fig. 7).

The functionality of the existing systems would be represented in an as-is simulation, as discussed above. The functionality of the existing systems instantiated as web services would be represented in a to-be simulation. Comparison of simulation results between the net-centric- and non-net-centric-enabled environments would allow an understanding of potential operational benefits from technology insertion.

Once decomposition is completed, sequential relationships can be established among process elements to convert the process decomposition into a workflow, which also can be modeled and executed. Figure 8 shows a notional workflow of a GS process that has been restructured and linked via an instrumented interface to a version of the planning tool. The blue boxes in the diagram represent notional lower-level process elements. The numbers in each box represent the time to complete the work associated with each process element in hours.

To determine whether our MRMEF approach is a viable means for evaluating C2, we focused an IRAD effort at APL on the use of the workflow model to help

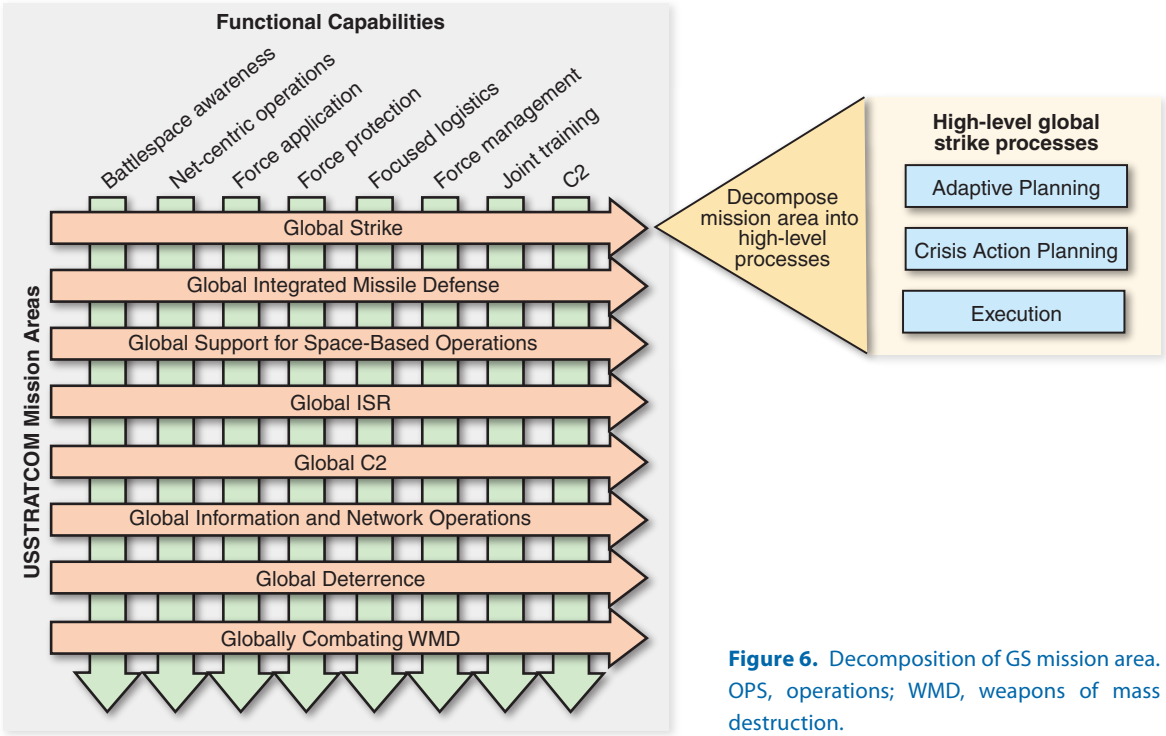

Figure 6. Decomposition of GS mission area. OPS, operations; WMD, weapons of mass destruction.

evaluate decision quality during the conduct of a typical strike process. The model characterized the activities and associated capabilities of that process, including activity completion times. It represented the sequencing relationships among the process elements in the form of a workflow. Execution of the model drove a visual representation of workflow completion status in the planning tool, which was used to synchronize the actual conduct of the planning process by participants in response to a scenario-driven experiment. The model also was used to record decisions made by experiment participants regarding the quality of the data to which they were exposed and whether those data supported the mission represented by the scenario.[4] Our experimental results demonstrated that the executable workflow model and supporting evaluation methodology served as an effective means for evaluating C2 processes.

OPERATIONAL C2 PROCESS INSTRUMENTATION

In an operational-level command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) system, such as a USAF CAOC, warfighters develop and disseminate C2 decisions and guidance based on an understanding of "what is happening." A typical CAOC is shown in Fig. 9. **ISR** provides location and status of military objects. **Computers** provide

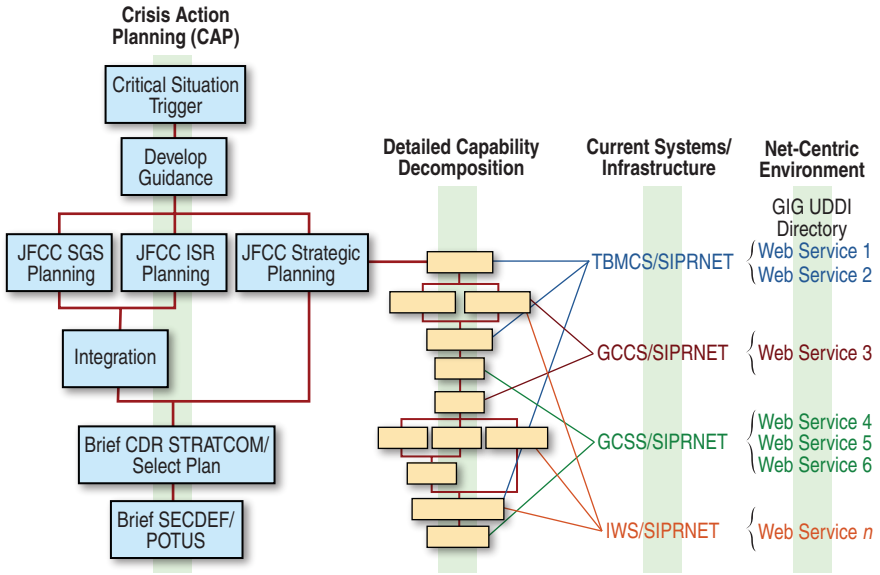

Figure 7. Mapping of process elements to systems and potential web services. GCCS, Global Command and Control System; GCSS, Global Combat Support System; IWS, InfoWorkSpace; JFCC, Joint Functional Component Command; POTUS, President of the United States; SECDEF, Secretary of Defense; SGS, space global strike; SIPRNET, Secret Internet Protocol Router Network; TBMCS, Theater Battle Management Core System; UDDI, universal description, discovery, and integration.

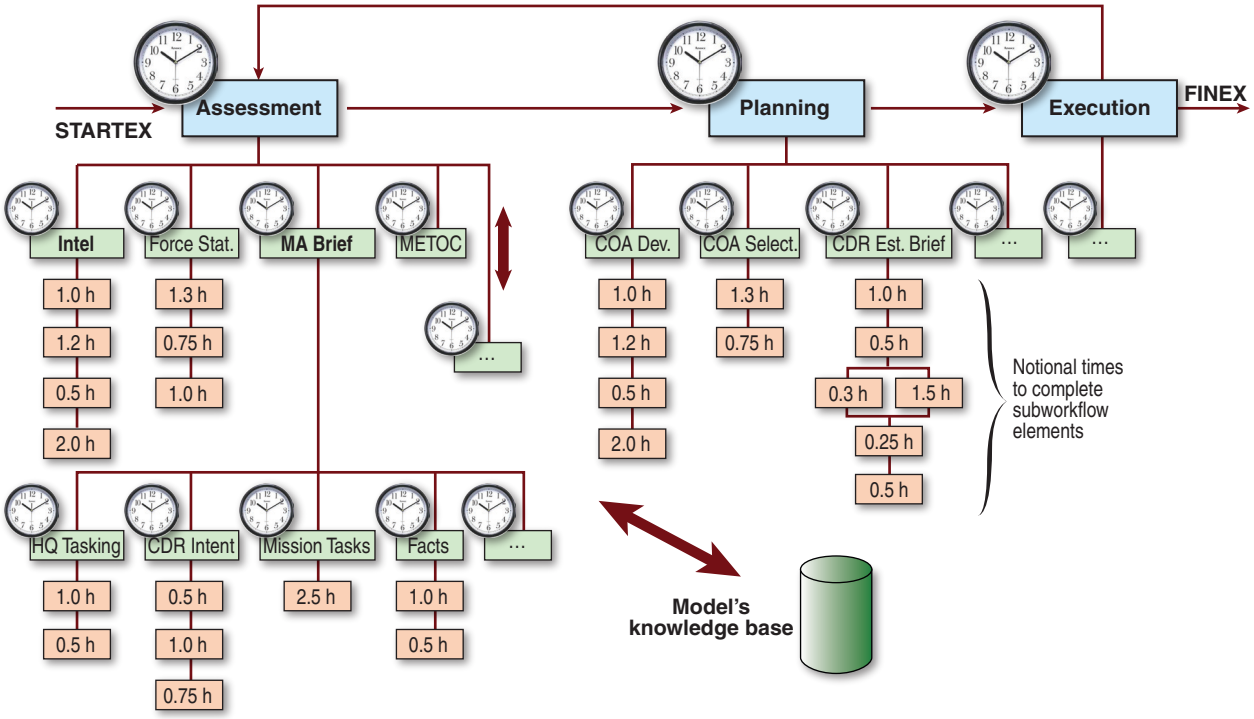

Figure 8. Executable GS workflow model linked to a Planning Tool. STARTEX and FINEX indicate the beginning and end of the process, respectively. CDR, commander; COA, course of action; Dev., development; Est, estimate; MA, mission analysis; METOC, weather; Select., selection; Stat., status.

the necessary software and hardware tools to facilitate decision making. **Communication** systems support collaborative activities and the distribution of decisions and guidance to warfighters. Together, these elements generate the shared battlespace awareness that enables effective C2.

Equally important to effective C2 is the need to understand "what has happened" and gather lessons learned. Unfortunately, in today's C4ISR systems, the majority of the data from the C4ISR elements are non-persistent. An enabling technology that addresses the need to reconstruct what happened is an Operational C2 Instrumentation System (OCIS). An effective and useful OCIS must collect and store data from all of the C4ISR elements including, but not limited to: where military objects actually were versus where decision makers perceived them to be; system loading, congestion, and downtime of the computer network and communications; the state and status of the computer systems; and, most importantly, the TTPs executed during the C2 decision-making process. Furthermore, an effective OCIS also must correlate, fuse, and portray the stored data as useful and meaningful information to the viewer.

Figure 9. C4ISR Center, USAF CAOC.

Under the sponsorship of the USAF C2 Battlelab and the USAF Research Laboratory, APL engineers, together with operational warfighters from the USAF 505th Command and Control Wing, created, prototyped, and installed an initial component of such an OCIS in multiple Air Force command centers. APL's CAOC Performance Assessment System (CPAS) is a process instrumentation capability that collects and stores time-sensitive targeting (TST) process data from multiple CAOC C4 sources. Concurrently, CPAS provides user-friendly displays to portray key TST process events and times overlaid on the kill-chain model, as well as metrics associated with numerous TTP process anomalies, in near real-time.

Currently, APL's CPAS process instrumentation technology is used to support warfighter readiness training, conducted during the USAF's premier operational training event known as Red Flag at Nellis Air Force Base. Using CPAS as an "after-action review" capability, TST instructors enhanced the quality of their post-mission analysis by reducing the time spent reconstructing what happened by 75%. Moving from the training to operational domain, the USAF Air Combat Command has endorsed the transition of CPAS technology into an operational-level C2 weapon system for the USAF.

NEW TRIAD ANALYSIS

During the Cold War, the strategic concept, consisting of bombers, intercontinental ballistic missiles, and submarines, was used to maintain strategic nuclear deterrence by guaranteeing the availability of a massive response to nuclear attack. The 2001 Nuclear Posture Review transformed the traditional nuclear triad of missiles, bombers, and submarines into a "New Triad," intended to guarantee that U.S. policymakers will have an appropriate way to respond to aggression, thereby bolstering deterrence.

With this transformation came an expansion of USSTRATCOM's mission, including global deterrence capabilities; combating adversary weapons of mass destruction worldwide; enabling decisive global kinetic and non-kinetic combat effects through the application and advocacy of integrated intelligence, surveillance, and reconnaissance (ISR); space and global strike operations; information operations; integrated missile defense and robust command and control.

Much of the nation's existing C2 system has been developed to support the old triad and a cold-war mindset that was centered on nuclear threats from nation-states and corresponding U.S. nuclear responses. In addition, a number of previous assessments (e.g., the Scowcroft Commission) have shown that the nation's existing NC2 capability has serious shortcomings that would make it a challenge to expand it to accommodate USSTRATCOM's New Triad missions.

As a result, USSTRATCOM and the nation as a whole must face the challenge of determining how best to transform a system with numerous single-purpose, stand-alone capabilities that were designed to support NC2 into an integrated system that is able to support the range of new triad missions against a variety of nation-state and non-nation-state adversaries.

In December 2005, APL was requested by the Assistant Secretary of Defense (Networks and Information Integration) to lead a study designed to answer the question of how best to transition the existing NC2 system to a New Triad C2 system. Because the results of this study are likely to have a significant impact on the future of the New Triad C2 system and, as a result, the safety and security of the nation, appropriate governance and oversight of the analysis was critical. This was provided by three separate bodies.

First, the APL team worked closely with a group of nearly 60 subject-matter experts (SMEs). These individuals represented a variety of interested government and military organizations, each with a key role in New Triad C2. This group was convened for 1–2 days approximately every 6 weeks during the study. During these meetings, the APL team presented results to date and received input and redirection, as appropriate.

The second group was the Analysis Senior Advisory Group. This group, composed of flag officers and Senior Executive Service government officials, was responsible for providing guidance and direction to the APL study team.

Finally, an APL "red team" was convened to provide guidance and review of the analysis process itself. This team was composed of former senior government officials familiar with the subject matter.

The study was organized as a modified analysis of alternatives consisting of several phases, as depicted in Fig. 10.

The first step in the study process was to understand the architecture alternatives. IEEE Std 1471-2000, "IEEE Recommended Practice for Architectural Description of Software-Intensive Systems,"[5] identifies architecture as the fundamental organization of a system embodied in its components, the relationships of these components to each other and to the environment, and the principles guiding the design and evolution of the system.

The IEEE definition highlights the importance of the components of the architecture and the relationships among them. With respect to NC2, components include various platforms, systems, communications links, and people. In addition to the components themselves, the relationships among them also are critical to defining and analyzing the architecture because communications is a key component of C2.

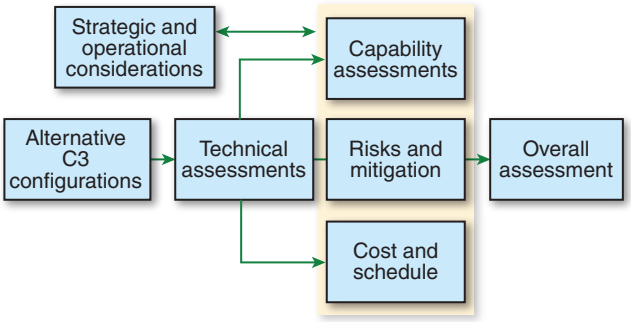

Figure 10. The APL analysis approach is a structural approach to analyzing and solving complex operational and technical problems.

The next step in the analysis was a comparison of alternative architectures, focusing on gaps, vulnerabilities, and limitations of platforms, systems, and networks on a day-to-day basis. Questionnaires were used to solicit information from military and government staff responsible for the operations and management of the various components of the NC2 system. In addition, information regarding NC2 functions supported by the components of each alternative was collected by using site surveys and during discussions with various organizations. This information was then used to map C2 capabilities to specific components.

In addition to understanding the architecture alternatives and the performance of the individual components on a day-to-day basis, it also was critical to understand the range of possible threats to the NC2 system. Using a variety of published intelligence reports, the APL team categorized the threat spectrum across a number of operational situations. The key to this portion of the analysis was to project a range of threats and operational situations under which each component of the architectures would be impacted, both individually and in combination.

Once the threats and vulnerabilities were understood, the team focused next on assessing the capabilities of each architecture alternative in various operational situations. Specifically, each alternative was evaluated in terms of a series of metrics. The metrics were survivability, endurability, accessibility, reliability/availability, timeliness, scalability, and assurability. This variety in metrics required that a variety of approaches and methodologies be used in the assessments. For example, a primary analysis tool for the capability analysis was the APL-developed Command, Control, and Communications (C3) Architecture Assessment Tool (CAAT). CAAT is a Monte Carlo simulation (implemented in Excel and Visual Basic for Excel) capable of generating multiple iterations in a single run.

Inputs to the model came primarily from the operational situations and architecture alternatives. However, in certain cases, where quantitative inputs were not available, sensitivity analyses were performed to assess the impact across a range of alternatives.

An additional focus of the capability assessment was an evaluation of the Internet Protocol (IP) network-based portion of the architecture. A performance assessment of the IP portion of the New Triad alternative architectures was conducted by using the OPNET network simulation to evaluate the following: (*i*) throughput, i.e., the average transfer rate of information from sender to receiver; (*ii*) the message delivery ratio, i.e., the ratio of transmitted packets that are received; and (*iii*) end-to-end delay, which measures the time of packet transmission from the originator to packet receiver.

The assessment methodology involved developing end-to-end connectivity diagrams for the proposed architectures and for each operational scenario along with information exchange requirements derived based on New Triad requirements outlined in various government documents.

Another key area of capability analysis was the level of information assurance (IA) provided by each of the alternative architectures with respect to computer network operations. The following criteria were used to assess IA:

- *Availability*. Confidence that authorized users have timely, reliable access to data and information services
- *Confidentiality*. Confidence that information is not disclosed to unauthorized individuals, processes, or devices
- *Integrity*. Confidence that the validity of information is protected

It often is difficult to quantitatively assess the effect of computer network attacks. There are no robust models available, and the results of the models that are available are highly dependent on the input parameters specified. Therefore, the process used for the assessment was centered on gaining insights and information from SMEs via a warfare analysis exercise or war game during which likely attacks, the ability to defend against those attacks, and the technical and operational impacts of the attacks if they did occur were all assessed.

The next phase of the analysis focused on risk assessment. This involved identification of the major risks associated with each of the architecture alternatives, assessment of the severity of each identified risk, and identification of potential mitigation options that could reduce the degree of exposure to each of the identified risks.

Two widely accepted components of risk severity were addressed in the risk assessment. First was the probability that a failure event might occur, which was referred to as "likelihood"; second was the potential for suffering an adverse consequence if that failure did occur, which was referred to as "impact."

The risk assessment was designed to address the following categories of risks:

- *Technical risk*. The risks associated with the evolution of the design, production, and supportability of the system affecting the level of performance necessary to meet the operational requirements
- *Cost risk*. The risk associated with the ability of the program to achieve its life-cycle objectives
- *Schedule risk*. The risks associated with the adequacy of the time estimated and allocated for the development, production, and fielding of the system

- *Programmatic risk*. Those risks that flow from or impose an impact on program governance, as well as those risks that impact program performance

- *Operational risk*. The risk associated with the ability to ensure that U.S. military and civilian personnel are ready at all times to accomplish the range of missions assigned to them in the defense strategy.

The risk assessment included three major steps. The first step was to identify the major risks associated with each of the architectures according to the various risk categories. Next was an assessment of the severity of each identified risk for each of the three time phases of the analysis as well as identification of potential mitigation options that could reduce the degree of exposure of the program to each of the identified risks.

A key component of the risk analysis was soliciting input from a panel of risk SMEs. These were government officials who were familiar with various programs and components of the NC2 system. Input was collected via a number of survey instruments in which SMEs scored the likelihood and impact of each identified risk. Collection and analysis of the risk survey responses were then performed by the APL Risk-Assessment Team.

The final step in the analysis was to assess the cost impact of each of the architecture alternatives. Costs were projected out to FY25 and were presented in both current-year and then-year dollars.

This analysis highlights APL's capabilities in architecture and analysis as brought to bear on a significant national issue. Furthermore, it highlights the APL's ability to bring together a multidisciplinary team from across the organization in a synergistic manner to address complex issues.

INFORMATION-SHARING ENVIRONMENT

The Intelligence Reform and Terrorism Prevention Act of 2004[6] calls for the President to create an ISE to improve and facilitate sharing of terrorism information. Subsequently, the President issued a memorandum that directed the development of a common framework for information sharing among federal, state, local, and tribal governments, and, where appropriate, with private sector entities and foreign allies, in a manner consistent with the protection of homeland and national security and with the protection of information privacy rights and other legal rights of Americans. In support of this effort, APL defined the approach to developing the architecture for the ISE, including a definition of the architectural views and artifacts that were to be provided. A unique approach was required because the ISE is a cross-enterprise effort, spanning the existing enterprise architectures of the participants. APL developed the approach and used it to define the initial version of the ISE EAF. The ISE EAF includes four primary views or partitions: the Business, Data, Application and Service, and Technical. Each of these is defined by a set of artifacts (technical drawings and descriptions).

Although the ISE is not generally thought of as a C2 system, it has as its core purpose the sharing of information to improve situational awareness and decision making, key elements of C2. The audience for this architecture includes the Chief Information Officers and enterprise architects of those federal, state, local, and tribal governments; private sector entities; and foreign allies that are participants in the ISE. Figure 11 illustrates the ISE concept. The vision for the ISE is to create a powerful new national capability to share, search, and analyze terrorism information. It will link information across jurisdictional boundaries and create a distributed, protected, trusted environment for transforming data into actionable knowledge. It will provide mechanisms to permit partner agencies at the federal, state, and local levels (e.g., fusion centers) to share data based on common standards.

The federal government has adopted an enterprise architecture approach to managing information technology investments. Each federal department and agency is required to submit an enterprise architecture

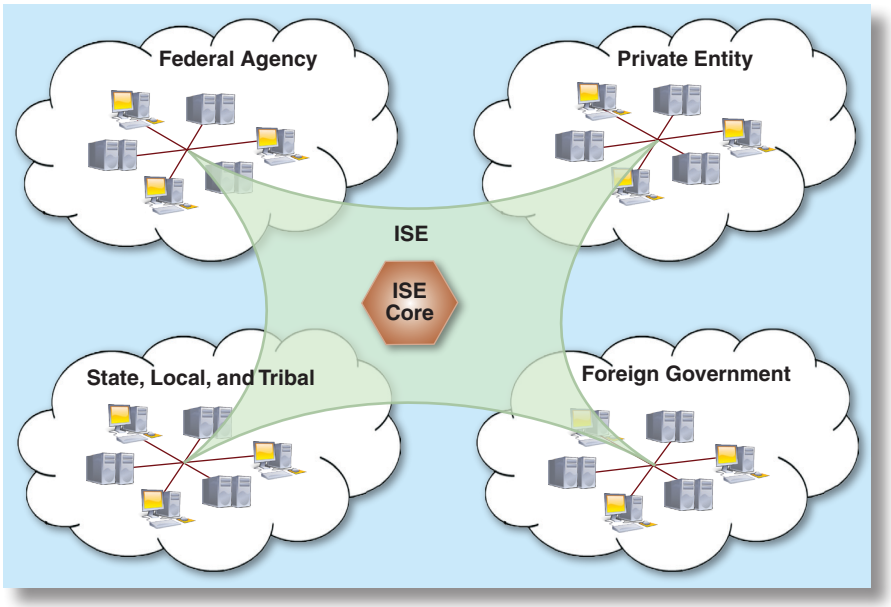

Figure 11. The ISE is a virtual environment to share terrorism information.

to the Office of Management and Budget (OMB) as part of the annual budgeting process. Each enterprise architecture must map its elements to the Federal Enterprise Architecture, a high-level set of reference models developed by the OMB. These enterprise architectures are beginning to improve information sharing *within* departments and agencies. The ISE is intended to improve information sharing *across* agencies and with external partners.

Current technology makes cross-enterprise integration possible and affordable. In the past, each agency had different technical environments that made integration dependent on building special-purpose interfaces and conversions among systems. The widespread adoption of IP-based communications, XML, web services, and associated platform-independent technologies has changed this situation. It is now possible to achieve integration at a basic technical level. However, an architecture is necessary to guide any cross-agency initiative to achieve this integration. The architecture must address issues in the areas of shared or cooperating business processes, common information exchange standards, data semantics, data quality, data volume, and IA. It is not sufficient to simply make all data available to anyone who might need it. This could result in an overwhelming flood of information that is no more useful to increased understanding than a lack of information. Sharing is not the end goal. Providing the correct information to support timely, informed decision making is the goal. Data must be protected from unauthorized access for privacy and security reasons. Data must be understandable. The huge volume of data that is potentially accessible requires tools to find and filter it to make it fit for use in a particular context. The architecture also must be a tool to promote common understanding among agencies in order to build trust and make the case for the policy and cultural changes necessary to allow and encourage information sharing.

APL developed the initial version of the ISE EAF, with a particular emphasis on the applications and services view (shown in Fig. 12). The architecture defines the major components, the relationships among them, and the unifying characteristics. Each agency will maintain its own independently developed and operated systems as defined by its enterprise architecture. However, each will establish an ISE Shared Space that is simultaneously part of its enterprise and part of the ISE. These ISE Shared Spaces, in conjunction with the Core Services and ISE Portal, provide the ability for users and systems within agencies to collaborate and share

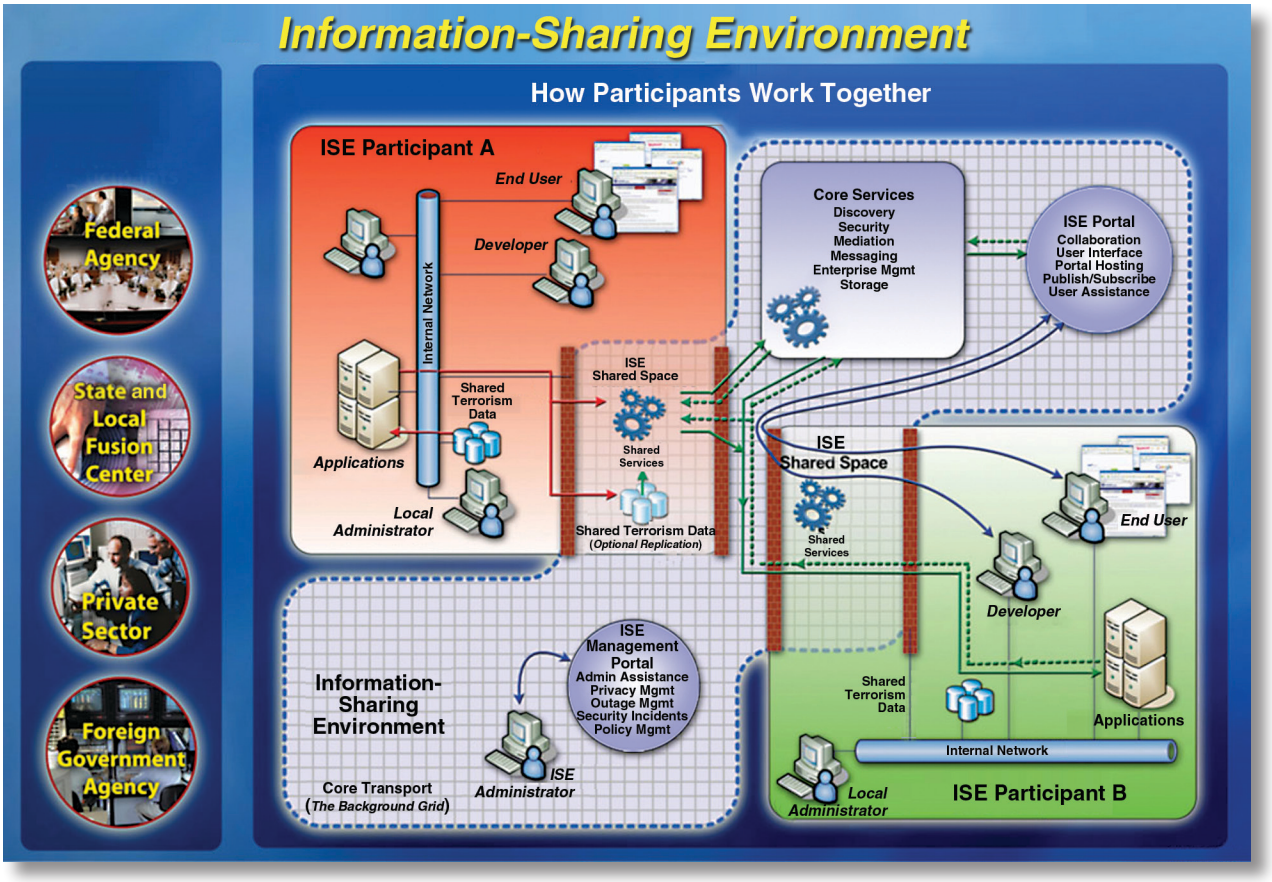

Figure 12. Overview of the ISE applications and services architecture.

information. The concept of the ISE Shared Space was critical to addressing the IA aspects of interconnecting the ISE participants.

SUMMARY

GED's C2 focus is to apply innovative technologies to our nation's C2 challenges. We are working with the DoD and other government agencies to fully leverage the GIG and net-centric implementation. We use a disciplined system engineering approach to understand both the advantages and limitations of these and other technologies. Incremental capability selection, piloting, and evaluation play an important role in our approach. We will maintain our focus on improving the C2 capabilities of our warfighters and first responders by understanding their processes and where technology can make improvements. Quantifying C2 performance is a cornerstone of our efforts: in constructive simulations, in distributed virtual test beds, and in live exercises. This capability can be used to evaluate the benefit of a proposed new C2 application or to provide feedback to operators during an operational exercise. Our goal is to make critical contributions to seamless C2 across all echelons of commands so that decision makers at all levels can achieve the desired effects on demand anywhere in our new national security environment.

REFERENCES

[1]The 9/11 Commission, *Final Report of the National Commission on Terrorist Attacks Upon the United States*, W. W. Norton and Company, New York, pp. 44–45 (2004).

[2]Alberts, D. S., and Hays, R. E., *Power to the Edge: Command and Control in the Information Age*, Command and Control Research Program, Washington, DC, p. 126 (2003).

[3]Alberts, D. S., and Garstka, J. J, *Network Centric Operations Conceptual Framework*, Version 2.0, Evidence Based Research, Inc., Vienna, VA, p. 15.

[4]North, P. D., "Use of an Executable Workflow Model to Evaluate C2 Processes," in *Proc. 12th Annual International Command and Control Symp.*, Newport, RI (June 2007).

[5]*IEEE Recommended Practice for Architectural Description of Software-Intensive Systems*, IEEE Std 1471-2000, The Institute of Electrical and Electronics Engineers, Inc., New York (2000).

[6]*Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)*, Section 1016, Public Law 108–458 (17 Dec 2004).

The Authors

Peter M. Trask is a member of the Principal Professional Staff in APL's Global Engagement Department. He came to APL in 2004 after working at the Naval Undersea Warfare Center in submarine communications and surveillance. He received a B.S. in electrical engineering from Northeastern University, an M.S. in electrical engineering from the University of Connecticut, and a M.S. in management from the Massachusetts Institute of Technology. His focus is on net-centric information integration and decision support and measurement of C2. **Frederic T. Case** joined APL in 1997 and is the Program Manager of the Operational Command and Control Program Area in the Precision Engagement Business Area. Mr. Case directs, manages, and provides technical contributions to several technology development programs focused on operational C2. He is a coinventor of the CPAS technology. Mr. Case is a former Defense Advanced Research Projects Agency (DARPA) Research and Development (R&D) Project Manager. While at DARPA, he managed and directed the activities of multiple advanced technology C2 and M&S programs. He holds an M.S. in systems technology from the Naval Postgraduate School, and he is a rated senior navigator with more than 1000 flying hours in fighter aircraft. Mr. Case is a member of the Military Operations Research Society and the Project Management Institute. **Steven L. Forsythe** is a member of the Senior Professional Staff in the Precision Engagement Systems Branch of the Global Engagement Department. He is currently on assignment in Dayton, Ohio, supporting Wright-Patterson Air Force Base. He holds a B.S. in physics from Kent State University and an M.S. and Ph.D. in operations research from the Air Force Institute of Technology. Dr. Forsythe is a retired Air Force Officer with expertise in C2, M&S, and optimization. **Thomas M. McNamara Jr.** is a member of APL's Principal Professional Staff. He is the Area Manager for the National Security Capabilities Program in the National Security Analysis Department (NSAD). He obtained a B.S. in ocean engineering from Florida Atlantic University and an M.S. in technical management from The Johns Hopkins University. His background includes expertise in undersea warfare, autonomous unmanned vehicles and systems, advanced R&D, DoD acquisition, systems engineering, and C2. His program area is focused on those Office of the Secretary of Defense and Joint Chiefs of Staff organizations that are tasked with assessing NSAD's capabilities for emerging national security challenges and strategically balancing and integrating joint defense capabilities. Mr. McNamara also was head of the Strategic Posture Office of APL, which coordinated APL's contributions to New Triad issues and strategic initiatives. **Paul D. North** is a member of the Principal Professional Staff in the Global Engagement Department. He holds a B.S. in biology from Saint Francis University, an M.S. in biology from Towson State University, and an M.S. in computer science from The Johns Hopkins University. He also holds a certification in Federal Enterprise Architecture from the California State University. His areas of expertise are technical management, information systems, and C2. **Kim E. Richeson** is a Principal Professional Staff member in NSAD. He holds a B.S. in engineering science from Purdue University and an M.S. in computer science from The Johns Hopkins University. Mr. Richeson first came to APL in 1968 and has had technical and management roles in a variety of application areas, including C2, commercial vehicle operations, management information systems, business systems, and radar detection and tracking systems. Mr. Richeson's recent work includes studies and prototypes related to strategic and national C2. He is a member of the International Council on Systems Engineering. **Christine O. Salamacha** is a member of the Principal Professional Staff in NSAD. She holds a B.A. in mathematics and an M.S. in computer science from The Johns Hopkins University. Over the span of her career at APL, Ms. Salamacha has worked in numerous different domain areas. The last 8 years, she has focused on C2, with an emphasis on distributed collaboration and support for senior leadership. **John J. Tamer** is a member of the Principal Professional Staff in the Global Engagement Department. He holds a B.S. in accounting from the University of Maryland and an M.B.A. from Syracuse University. Mr. Tamer joined APL in 1997 and is currently Group Supervisor of the Information Systems Engineering Group, where his work focuses on enterprise architecture development and evaluation. For further information on the work reported here, contact Peter Trask. His e-mail address is peter.trask@jhuapl.edu.

Peter M. Trask

Frederic T. Case

Steven L. Forsythe

Thomas M. McNamara Jr.

Paul D. North

Kim E. Richeson

Christine O. Salamacha

John J. Tamer

The *Johns Hopkins APL Technical Digest* can be accessed electronically at **www.jhuapl.edu/techdigest**.