INTEGRATION AND INTEROPERABILITY OF INFORMATION SYSTEMS WITHIN THE COALITION AEROSPACE OPERATIONS CENTER

Marvin L. “Lenard” SIMPSON, Jr.

Introduction

In any coalition operation we face a continuing challenge where we must strike a balance between classified information sharing among coalition partners and a requirement to protect each coalition partner’s information sources and collection capabilities as defined by each nation’s laws and regulations.

With that in mind, in order to maximize combat capability and reduce risk (fratricide, threat avoidance and suppression, inadvertent disclosure of sensitive data etc.) the operational commander and his staff must have access to the most accurate information in time to plan, act and react with confidence.

When information/data is stored, sorted and manipulated across several different Local Area Networks (LAN’s) and Wide Area Networks (WAN’s), each with disparate security levels and applications, we run the risk that critical information will not be available for use by the appropriate personnel in a timely enough manner to make the correct decision.

Unfortunately, current technology does not support automatic transfer and synchronization of massive databases across LAN’s and WAN’s with disparate security requirements. With that in mind, perhaps the answer is one master data set populated with the best information available and usable by all coalition partners. This master data set would be used to plan and execute the majority of coalition military activities. There is an inherent risk associated with this arrangement, which will be covered in this paper.

INFORMATION & SECURITY. An International Journal, Vol. 8, No. 2, 2002, 175-193.

CAOC Defined

A Coalition Aerospace Operations Center (CAOC) is defined for this paper as the location/organization (personnel, capabilities and equipment) through which the Coalition Forces Air Component Commander (CFACC) exercises command and control (C^2) of aerospace forces. It is the senior element of the Theater Air Control System (TACS).

The CFACC employs the CAOC to facilitate the maneuver and mass overwhelming aerospace power through centralized control and decentralized execution to produce desired operational and strategic effects in support of the Coalition's campaign. Infrastructure, systems, processes, and training should be shared and integrated to the maximum extent possible while ensuring that the integrity of all military missions is maintained. The design should maximize interoperability while promoting the independence and flexibility necessary to support complementary—but not identical—missions executed under nominal conditions.

Assumptions

The CAOC functions at the coalition/component level and provides the CFACC with the capability to direct and supervise the activities of assigned, supporting, or attached forces, and to monitor the actions of both enemy and friendly forces. In order to function, the CAOC requires connectivity to operations centers of higher service/joint/coalition headquarters, lateral headquarters, and subordinate units. This allows for the continuous collection and presentation of battle management information. CAOC personnel, in accordance with the priorities, objectives, and strategies, conduct detailed direction of all aerospace operations by using this data.

To lay out a proposed methodology for a notional CAOC, several assumptions have to be made. It will be assumed that the Coalition commander exercises command over the Coalition command, control, communications, and computers intelligence (C^4I) information and processes system. The Coalition will use its C^4I System to plan, direct, coordinate, and control the various aspects of Coalition operations. These missions could include but are not limited to:

1. Maintain continuous surveillance of the Area of Responsibility (AOR) aerospace to deter hostile states from entering the AOR.
2. Effectively employing assigned forces in defense of the AOR should deterrence fail.
3. Planning, directing, monitoring, and controlling air operations while providing C^2 support to assigned forces and other military and civilian agencies.

4. Integrating their operations with other C^2 systems to form a coherent structure for joint and combined operations.

Processes

The primary processes used in our notional CAOC will be the same as used by current AOC’s, which are:

1. Planning

Aerospace planning processes will focus on the desired strategic and operational effects the CFACC is to produce. These desired effects will be articulated in courses of action (COAs). Once a COA is selected, the effects the CFACC is tasked to produce will be specified. The aerospace strategy is the CFACC’s concept for employing aerospace capabilities to achieve objectives in support of the overall campaign. The “means” will be kinetic and/or non-kinetic use of aerospace power. Since aerospace power is a theater-wide instrument, CFACC planners must be involved in the development of other coalition member COA options. This integration of plans constitutes three, highly iterative and interactive, sub-processes. One is developing support requirements those components foresee from the aerospace component. The other is the support requirement that the aerospace component foresees from other components. A third— and perhaps the most important— sub-process is gaining an understanding of the mechanism each component foresees on how their COA helps accomplish the overall battle objectives. Integration of efforts between components occurs on multiple levels requesting aerospace support. The focus here is integration of the CFACC’s planners through the execution and assessment process to maintain a long-term focus concurrently with the other components/ coalition member country.

Based upon changes in the situation, direction or resources, planners will develop daily CFACC guidance for approval and dissemination. Guidance, translated into prioritized aerospace tasks, provides the necessary information to begin the target nomination process. The targeting process is the linkage between guidance and application. Targets are nominated based on this guidance, intelligence recommendations, component requests, and other factors. Resources are then allocated to accomplish specific missions. Packages are constructed to maximize the effectiveness of available assets. The Master Air Attack Planning cell (MAAP) provides specific guidance on how daily aerospace operations will be conducted. The MAAP provides theater-level sequencing and resource inputs necessary for producing an ATO and is the first time in the aerospace tasking process that detailed resource availability is matched against specific targets to achieve desired effects. Working closely with specialty teams, component liaisons, and unit representatives, the Integrated Prioritized Target List, threat situation, joint prioritized collection, forecast weather, weapons system availability, air refueling, and weapons employment options are synchronized. The MAAP has sufficient flexibility to adapt to the changing battlefield situation throughout the theater.

After the MAAP's plan is approved by the CFACC, detailed preparations continue with the production of the ATO, Special Instructions (SPINS), and Airspace Control Order (ACO) using CFACC guidance, target worksheets, and various component inputs. The Airspace Control Authority and Area Air Defense Commander instructions provide sufficient detail to allow components to plan and execute all missions tasked. These directions enable combat operations without undue restrictions, balancing combat effectiveness with the safe, orderly, and expeditious use of airspace.

2. Execution

Even a perfect plan requires adjustment during the execution phase of conflict. Execution comprises steady state and dynamic functions enabling the CFACC command of continuous, rapid, and dynamic aerospace power. The CFACC commands aerospace power across the spectrum of conflict by directing, controlling, monitoring, and assessing forces under his tactical control. The CFACC will maintain battlespace awareness, which is essentially situational awareness at the operational level. Battlespace awareness will provide an accurate picture of friendly and enemy operations within the area of interest and is the key enabler of the CFACC's ability to command in real time. It also provides the capability to view and monitor emergent threats and potential targets giving the CFACC the ability to redirect assets during execution. Key data and information links will be from, as a minimum, in-theater and national level sensors, tactical data links, and messaging at all levels to provide relevant information available for execution. Battlespace Awareness, in a Common Operational Picture (COP) for example, combines information from air, surface, subsurface, ground, and space assets to provide a three-dimensional view of the battlespace. Sensor and data fusion within this picture plays an important role in validating targets and eliminating ambiguous information.

3. Continuous Assessment

The CAOC will monitor enemy and friendly actions and reactions; identify potential threats, weather and its impact to friendly forces/operations, and subordinate unit combat reports/logistics status. During execution, each functional area will continuously monitor changes to the plan. This information provides a comprehensive picture of current and projected capability, and is tailored to the needs of the CFACC. In addition to speeding up the decision making process, this "quick look" picture facilitates proactive command of aerospace operations. Developing this level of situational awareness should not inundate decision makers, but rather give them information needed to command/control the fight, and answer the CFACC question, “What’s the enemy doing and what options/capability do we have at this point?” As unexpected/unplanned events occur which affect the plan (e.g. strike package delays), combat operations will assess impact on their own functional area, the impact on the current operation, level of reporting required, and then develop options for the decision maker. Changes must be communicated horizontally to other planners, and vertically to tactical units and other headquarters. Continuous assessment often reveals a “trigger event,” that can launch combat process.

Current Information Protocols

Foreign Disclosure Officers

Foreign Disclosure officers are the personnel in the US CAOC responsible for implementing the National Disclosure Policy (NDP) that governs the disclosure of United States Classified Military Information (CMI) to foreign governments and international organizations. CMI is under the control of the US Department of Defense. Access to CMI is based on the impact to national security. It is designated as TOP SECRET, SECRET or CONFIDENTIAL. Foreign Disclosure officer responsibilities include: Knowledge of specific disclosure criteria and limitations, definitions of terms, and other guidance governing decisions on the disclosure of CMI.

Under conditions of actual or imminent hostilities, any Unified Commander may disclose CMI through TOP SECRET to an actively participating allied force when support of combined combat operations requires it. The U.S. Commander must notify the Chairman of the Joint Chiefs of Staff (JCS) of such disclosures. The Chairman of the JCS, in turn, must notify the Office of the Under Secretary of Defense for Policy, who will determine whether any limitations are necessary on continued disclosure of the information.

Current Automatic Assurance Guards

Current automatic information assurance guards are similar to the Defense Intelligence Agency -certified Imagery Support Server Environment (ISSE) Guard, developed by Rome Laboratory. The ISSE Guard provides a secure interface for the direct soft-copy exchange of information between Top Secret Special Compartmental Information (SCI) systems and Secret Collateral systems operating over strategic and tactical wide or local area networks. The Guard consists of the Common Guard Interface (CGI) application, hosted on high side users’ workstations and the Guard application running on the B-1 certified CyberGuard Night Hawk platform. The Guard is a bidirectional guard supporting the high to low and low to high transfer of e-mail and image files and the high to low transfer of text files. The ISSE Guard currently has two external interfaces: a high side Ethernet (IEEE 802.3) interface and low side interface that can be either 802.3 or X.25. ISSE Guard provides the functionality required to securely connect, validate, downgrade and transfer information between systems and networks operating at different security levels, while the CGI provides high side users with an interface to the Guard.

Imagery Support Server Environment Guard version 3.0 permits the secure digital exchange of electronic mail, imagery, text, and multimedia information between networks operating at dissimilar security classification levels. The system provides the ability to electronically connect networks operating at dissimilar security classification levels and supports the seamless, high-speed, controlled flow of information across security domains. This version provides significant increases in performance (an increase in throughput rate from 1.3 MB/second to 3.4 MB/second, a standards based open systems oriented Guard application, and a more stable and secure trusted interface). Future plans include hosting the Guard application on a Trusted Solaris platform and migration to Defense Messaging System (DMS) functionality.

Current Access to Data Repositories

In today's environment, the ability to gather information on a "particular item of interest," requires a user to log into each of the data sources using a unique interface for each source. Once logged in, the user must be cognizant of the interface for the source they are using to gather information. While the concept appears straightforward, it requires the user to be very knowledgeable with the various systems. In addition, it requires developers to spend an enormous amount of time and money designing/implementing these unique client interfaces for each data source. Improving data access is the mission of Broadsword.

Broadsword is a secure web-based application, which provides improved access to Department of Defense data repositories. Broadsword provides users simultaneous access to multiple and geographically separated data sources through employment of a web browser. Broadsword accomplishes this by deploying middle-ware translators know as Gatekeepers. These Gatekeepers take a single, simple or complex search criteria from a Broadsword user and translate this search criterion into native queries supported by legacy data sources. Gatekeepers then consolidate the responses of the disparate data sources into a single response, and return it to the Broadsword user. Broadsword is designed for employment across the spectrum of operational and security environments.

Broadsword especially benefits users at locations lacking robust command and control, communications and intelligence resources. Leveraging the power of web-based computing, Broadsword users need not be at the same physical site as the data repositories they need access to. Instead, Broadsword provides users the ability to access data remotely by accessing their home unit Gatekeeper and retrieving only the latest updates. Conversely, rear-echelon analysts using standing profiles and file transfer protocol (FTP) processes between Gatekeepers may push the data.

Broadsword employment is tailorable to organizational mission, unit function, and personnel task level. Broadsword's core ability is to improve data access.

System Certification and Accreditation

Generally, US coalition computer-based information systems and LAN are designed and developed to meet the Secret and Below Interoperability (SABI) requirements and all local site accreditation requirements as set by the Designated Approval Authority (DAA). Based on guidance from the project's SABI Customer Advocate, a proposed system should then anticipate the SABI/accreditation process to include system profiling by National Security Agency. If the proposed technology has not been previously approved as a SABI Reference Implementation (SRI), than the development will be executed as a New Technology effort under the SABI process. Detailed guidance for system certification and accreditation effort would then be provided by a SABI Customer Advocate team. It should be readily apparent that any program that qualifies for the SABI process and a SABI Customer Advocate would be time consuming and manpower prohibitive to design and develop.

The SABI requirements could call for the use of the tailored SABI version of the DoD Information Technology Security Certification and Accreditation Process (DITSCAP), Systems Security Authorization Agreement (SSAA). The SSAA includes two parts, an Executive Summary and a list of appendixes that are the technical and policy documentation for the C&A process. In addition to the documentation specified in the SSAA, the proposed system would have to recommend the following technical requirements and design documentation:

- Security Policy
- Functional Concept of Operations (CONOPS)
- System Functional Requirements
- System Functional Specification
- System Top-Level Architecture and Design

A detailed Coalition CONOPS should be written in the early planning stages of any experimentation. The CONOPS should document the assumptions and general approach to be taken toward creating that specific coalition environment. The CONOPS should become part of the accreditation package.

No means have yet been identified to permit collaboration on a data network across security domains. A real attempt to build an open floor CAOC with non-US personnel as full partners will require significant funding and an increase in staff to implement disclosure and security policy.

To maximize the chance for success, timelines for obtaining accreditation should be observed. DAA initial accreditation actions normally begin not later than 150 days prior to network activation. Non-standard security solutions (firewalls/routers, new guards) cannot be implemented in a short timeframe. Extensive testing by national agencies requires long lead times. Long-term funding could be a consideration for this type of large-scale effort.

Current Security Architecture Challenges

Highest Common Security Level Network

The US Command and Control (C^2) computer system, Theater Battle Management Core System (TBMCS), will be used as an example to illustrate this type of network. Unfortunately, US C^2 computer systems in general cannot easily support coalition operations due to disparate data security requirements. However, one option when using a C^2 system like TBMCS would be maintaining required databases, producing message sets and executing coalition operations on a 'highest common security level network', i.e. the highest classification/level data that can be contributed by each partner without violating their laws and regulations.

There will be certain functions (such as the plans and locations of individual nation's special operations forces or stealth aircraft mission planning requirements) that require individual nations to procure, manipulate and disseminate data separately from the coalition network to avoid inadvertent disclosure of sensitive data as decreed by law or regulation. There is an inherent risk associated with this and it will be covered in the next section.

Acceptable Risk?

There are risks that must be addressed and accepted when a nation attempts to reduce the chance of compromising national secrets and capabilities by operating autonomously in a coalition environment.

An example will be given. "Nation X" has an aircraft whose mission planning requirements require the use of data that is classified "Nation X Only" or perhaps the mission planning process exposes certain vulnerabilities of the weapon system that

“Nation X” does not want disclosed to certain members of the coalition. To protect it’s asset and subsequent data, all mission planning is conducted in a “Nation X Only” environment or enclave, separated from the rest of the coalition partners.

Let us assume this aircraft requires support from coalition resources (aerospace, tankers, EW support aircraft, etc.) to conduct it’s mission. The “Nation X” enclave is plugged into the coalition network on a separate terminal, has access to this information and uses it in it’s mission planning.

Unfortunately, the folks who are doing the coalition planning and monitoring the mission execution of their assets do not know the support requirements of “Nation X’s” aircraft and have modified the route, time on station or coverage of the support assets that “Nation X’s” aircraft is relying on to execute it’s mission. Because the planning for this mission has been executed outside the coalition environment, “Nation X” has put at risk the very assets they are trying most to protect.

On the positive side, there are workarounds utilizing a TBMCS-based coalition network, but these require additional manpower. The required additional manpower is diametrically opposed to the reduced footprint goals we have established to lessen our force protection vulnerabilities.

Highest Security Level Network

Today, the preponderance of stealth or special mission aircraft and their associated ‘special access program’ mission planning requirements and vulnerabilities belong to the US. Also, most of the collection platforms are classified ‘US Only’ whose capabilities are guarded by US law and regulations. Because of this, the operational commander may select the option to have master data classified as US Only. Generally, this option requires significantly more US manpower. If the C^2 databases are on the US Only side, the full functionality of TBMCS can be used and information within the individual applications can be populated with the most precise ‘US Only’ classified data available. Current technology will allow the ATO/ACO and other required message sets to be produced and delivered to coalition partners. Unfortunately, this can lead to mistrust among coalition partners – especially those that don not have similar assets and restrictions placed on what they can share in a coalition environment.

No Databases

The third option that could be considered by the operational commander, with due diligence, is not to populate the large C^2 organic databases. This option would be necessary in the case that there is not enough time to adequately train, or manpower (coalition or US) available, and systems are non-available. US C^2 systems are designed to operate in a joint environment with many processes going on unseen by the operator. Example: In TBMCS, to populate the AODB with friendly fire units so the operator can see the location of the units when the Friendly Order of Battle (FROB) is queried, TBMCS must receive a B220 message from the Army's Advanced Field Artillery Tactical Data System (AFATDS).

The no database option is measurably less efficient due to the fact that improvised procedures must be developed and learned by all partners. This "fall back" position does have the advantage that generally Commercial Off The Shelf (COTS) software is used in conjunction with Management Information Systems (MIS) products on a common LAN. This methodology is not the most efficient, but it allows coalition partners to be engaged in the planning and execution from the start of the operations. Operational Commanders should be completely aware of all consequences and limitations caused by selection of this option, including the significant increase in manpower required.

In any operation there may be a mix of all three options as the Commander attempts to mitigate risk and improve combat effectiveness.

Experimental Methodology

To achieve greater opportunities for enhanced mutual interoperability and capability, liaison elements from both the Coalition and US Forces should operate in a collocated area within the area of responsibility (AOR). The composition and functionality of the US initial cadre operating in the AOR, working with their Coalition counterparts, should be responsible for developing processes and procedures to implement integration/interoperability initiatives validated through experimentation.

Moreover, a Coalition liaison element comprised of 20 – 30 personnel should operate from the US, dispersed to appropriate functional areas to operate "side-by-side" with their US counterparts.

EXPERIMENTAL METHODOLOGY (Coalition Information Architecture)

In December 1999, Air Staff and the Defense Intelligence Agency approved the requirement to allow high-side (a more secure network) war fighters to see low-side sources (a less secure network) (e.g. Air Order of Battle Database (AODB)), query them and request products to be delivered to the high-side user (e.g. Situation Assessment Analysts). Coalition Information Architecture (CIA) should expand this requirement to allow a reverse (reach up) capability.

CIA could act as the umbrella initiative to provide automated multi-level security data sharing to support coalition interoperability between Joint World-wide

Information Communications System (JWICS), SIPRNET, NIPRNET, a Coalition Wide Area Net, and theater specific LAN. Functionality should reside within the CIA infrastructure without needing to build an independent infrastructure. This capability should augment existing C^2 systems, not replaces them. CIA encompasses the benefits of Broadsword and ISSE Guard by adding the Trusted Transfer Agent (TTA).

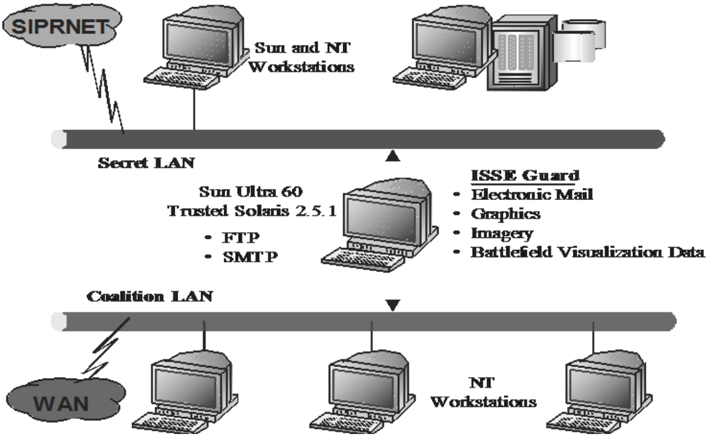

Figure 1: ISSE Guard Functional Architecture

The TTA program leverages the strengths of Broadsword and ISSE Guard to enable Multi-Level Security (MLS) information access. TTA brings together this powerful infrastructure and the multiple security level capability provided under the ISSE Guard. In order to ensure that high side information is not inadvertently passed through the TTA and ISSE Guard to the low side, two levels of extensive security filtering capabilities are provided: message level filters and field level filters.

Messages level filters use a “dirty word” list containing a list of words and/or phrases that are either not passable to the low side (e.g. classified code words, etc.) or strong indicators that the associated information in the message is not passable to the low side (e.g. security labels). By applying the message level filters it is determined if a message being passed through the TTA (and subsequently the ISSE Guard) from high to low contains any “dirty words”. If a message is found to contain one or more words/phrases in the dirty word list, the processing of the message is terminated. Field level filters are an additional capability added to the TTA. Since the messages passing from high to low through the TTA contain formatted field-value pairs, additional filtering can be provided on a field-by-field basis. For each field within each message type, over which field level filter is needed, an entry in a file is generated describing how the information in the field is to be filtered. A variety of filter types have been created which test for conditions such as Value in Field, Value Not in Field, Value in Range, etc.

When individual applications like ISSE Guard, Broadsword, and TTA are used on CWAN, users from various countries can become one effective fighting force. These users will be able to exchange e-mail messages with the Secure Internet Protocol Router Network (SIPRNET) users via the ISSE Guard. Additionally, Coalition users will be able to access various power point briefings, ATOs, and other large files via a web server located on CWAN. Web site content managers will replicate the web site residing on CWAN and SIPRNET web servers to corresponding web servers. This replication process will permit Coalition and US Forces access to identical web sites with content releasable to Coalition partners.

During operations, record message traffic could become backlogged, and the delay could create difficulties for coordination and execution. Message traffic could be posted to the local web server, thus providing much faster access. A word of caution – E-mail is a useful tool for coordination, but large e-mail attachments, such as an ATO being “pushed” to all Coalition tactical level users, could severely affect naval ships or other tactical users with low bandwidth capability.

One of the goals of the CAOC should be to provide access to Coalition information for all Coalition partners via a common web site. To achieve this goal, C^2 should be established on a CWAN that will link non-US combined forces to e-mail and web services hosted by the CAOC. A secure mail guard (e.g. ISSE Guard) should allow US personnel to access e-mail and other web services via SIPRNET, and at the same time allow information posted to the common web site to be releasable to all coalition partner countries. Current web site technology should be used to distribute and collect operational information.

The web site should function as a “digital binder” and contain planning documents such as Rules of Engagement (ROE), Schedule of Events (SOE) and periodic reports/orders such as Commander’s Intentions, Operational Reports (OPREPS), and standard United States Message text Format (USMTF) message sets like the ATO/ACO. The Coalition Commander would provide guidance to his forces through documents posted on the common web site. These documents could be in any form that can be displayed on a web site.

The goals of the Coalition Web Site should be two-fold:

1. To provide intelligent, timely and relevant information and knowledge on operations and intentions from subordinates to superiors and from Tactical Force Commanders to the Coalition Commander.

2. To provide a means for all military forces to exchange significant tactical and operational information in hopes of ultimately replacing message traffic.

Interoperability Opportunities

Operational processes that have a potential to be readily integrated are: air picture, theater missile defense notification, ATO integration (common message sets), secure communications systems and data networks, intelligence distribution, and common weather picture.

Common Operating Picture

The term, Common Operating Picture or COP, is one of the most misused words in today's C^2 vocabulary. As a result, C^2 warfighters, staff representatives, and technologists frequently face a great deal of confusion in trying to discuss the concept, employment, utility, and evolution of the COP. Much of this confusion can be resolved through reference to Chairman, Joint Chiefs of Staff Instruction (CJCSI) 3151.01, Global Command and Control System Common Operational Picture Reporting Requirements. It defines COP as an information tool supporting the warfighting CINC. It further defines the Common Tactical Picture (CTP) as an information tool supporting the Joint Task Force. In general, CJCSI 3151.01 describes the COP/CTP as a tool that provides battlespace awareness through a variety of information domains including, "current, anticipated, or projected, and planned disposition of hostile, neutral, and friendly forces." The COP/CTP may also depict logistics, readiness, planning, as well as other data to support Commander-in-Chief and coalition operations. Although the instruction makes reference to Component participation in feeding/maintaining the COP/CTP environment, it does not define or describe how the Components will participate in that activity.

(US) TBMCS/SAA and (Coalition) TBMCS/SAA could be dynamic tools providing users and COP Masters/network administrators options in supporting higher headquarters commanders and their subordinate units. (US) COP/CTP would provide every user within a designated network the ability to see the same Near Real Time (NRT) picture. (Coalition) COP/CTP would provide every coalition user within a designated network the ability to see a limited NRT picture. In doing so, it also provides each participant the ability to update, add to or corrupt the NRT picture the entire network (AOC on down) sees. Given this, COP Masters must implement a stringent set of guidelines and procedures. Most importantly, COP Masters must ensure that each participant in the COP is thoroughly trained on the system. COP/CTP Masters must establish and enforce a set of rules that balance user requirements against the COP Masters' need to ensure against data loss and/or corruption. A process of database synchronization is used to accomplish the transmission of data to the COP on a single LAN.

RADIANT MERCURY is a software application developed under contract to the Navy, which can automatically sanitize and downgrade formatted classified documents and synchronize a (US) COP/CTP with a (Coalition) COP/CTP. RADIANT MERCURY operates according to predefined security rules. The automation of the sanitization and downgrade process decreases the time needed to perform these functions, and eliminates human error.

Once an authorized node is brought into the COP/CTP, the entire track database is copied from the SAA (US) or (Coalition) server onto their nodes Track Data Base Manager (TDBM)(US) or (Coalition). New reports and track updates received by the COP/CTP Master are copied onto client nodes as the tracks come in from NRT sources. Updates, deletes, and modifications to data in the COP from client nodes are copied to the COP/CTP Master server/terminal at regular intervals.

However, the technical solution once implemented, will provide a common operating picture to the maximum extent possible that each country authorizes for release. Viable integration and interoperability of US and Coalition air pictures, procedures, and equipment can be achieved through the following:

1. The US should provide personnel in the CAOC to work with Coalition counterparts to reconcile dual tracks and other link management issues.
2. Coalition members, on a case-by-case basis, should jointly produce documentation referencing operational procedures for the combined data-link network.
3. US Forces and Airborne Early Warning aircraft (E-3 and E-2) can use Coalition sites as their primary TADIL-A ground entry station (GES); but other GES locations may be used as necessary.

The term Air Component Picture (ACP) is defined as the integrated battlespace picture derived from sources managed by the Aerospace Component. As a subset of the CTP and COP, it establishes the aerospace portion of the COP's battlespace infosphere. The ACP data may contain real-time or near real-time battlespace information; aerospace component planning information; aerospace logistics and readiness information; as well as relevant information distributed down from the C/JTF CTP or horizontally from other component's pictures. When properly managed, the ACP will provide dominant battlespace knowledge to synergize the command and control of the Aerospace Forces in support of combined operations.

The ACP is a powerful information tool, providing access to several information domains pertinent to aerospace operations. Readers should note that the COP, CTP and ACP software are virtually identical. The difference in the three terms include level of employment (e.g., strategic, operational, tactical), focus on organizational functions, and the manner in which the information is processed for decision-making.

Theater Missile Defense Notification

Theater Missile Defense (TMD) functions, within the defensive operations branch in a CAOC, fulfill the roles of passive and active theater missile defense. Additionally, this function works cooperatively with the Intelligence to determine enemy theater missile areas of activity/interest for further exploitation. The TMD function may have space and intelligence liaison representatives manning specialized equipment consoles for passing missile launch and impact point alerts. They also search for areas of interest for further reconnaissance exploitation and possibly eventual creation of either a time critical or standard target process.

The defensive operations branch is separated into three primary interconnected functions. These functions are air-breathing threat for fixed and rotary wing assets, theater missile defense for passive and active defense, and link management control, to provide an accurate consolidated air picture. Air Breathing Threat function is what many people think of as the traditional role of air defense. This function manages defensive fighters and surface to air missile defenses in direct support of the air defense mission. Defensive Duty Officer (DDO) evaluates and recommends changes in air defense activity, airspace management, and surveillance performance. He sits on a console displaying the air picture and remains in contact with subordinate units. Duty officers for specific coalition aircraft or missions may be available to assist in coordinating defensive operations. The DDO with the help from air defense liaisons coordinates air and missile attacks against threatening enemy air targets. The DDO could potentially receive time sensitive information from a common voice net (Voice over IP) that could be used for tactical dissemination and response.

Standard Message Sets

The Defense Information Systems Agency (DISA) is responsible for maintaining US Department of Defense information technology standards and conventions. Within DISA, the Center for Standards is the designated configuration manager for the United States Message Text Formatting (USMTF) Program. The USMTF Program documentation consists of two major documents, MIL-STD-6040, United States Message Formatting Program, and CJCSM 6120.05. To use military diverse forces effectively, a continuing need exists to increase the fighting capability through compatibility among the various C2 information systems and interoperability at the information level. This is done through the adoption and maintenance of standards and systems designed to provide interoperability through the use of approved joint data and information exchange standards. The operational benefits gained by allied forces from the use of common or compatible C2 standards are essentially identical to those for U.S. forces engaged in joint operations. In the combined environment, an additional advantage is the alleviation of information exchange problems associated with differing national languages and military organizational structures. Because of the large United States investment in tactical C2 systems the USMTF is the most logical interoperability standard that should be used in message sets. An example of two USMTF message sets used in the CAOC would be the Air Tasking Order (ATO) and the Air Control Order (ACO)

Electronic Mail (E-Mail)

Let us examine how to handle e-mail in a coalition environment. It is often impractical to maintain a message transport system on certain types of smaller C2 nodes. For example, a workstation at a tactical unit may not have sufficient resources (cycles, disk space) in order to permit a Simple Mail Transportation Protocol (SMTP) server and associated local mail delivery system to be kept resident and continuously running. Similarly, it may be expensive or impossible to keep a tactical personal computer interconnected to an IP-style network for long amounts of time (the node is lacking the resource known as “connectivity”). Despite this, it is often very useful to be able to manage mail on these smaller network nodes, and they often support a user agent to aid the tasks of mail handling. The Post Office Protocol – Version 3 (POP3) is intended to permit a workstation to dynamically access a mail dropped on a server host in a useful fashion. Usually, this means that the POP3 protocol is used to allow a workstation to retrieve mail that the server is holding for it. The well understood commercial standard of POP3 would most likely be used during any coalition operation. The problem that needs to be understood is difficulty in transferring e-mail between networks of various levels of security.

A secure coalition e-mail system generally utilizes a high assurance guard system (ISSE Guard) to permit exchange of e-mail without attachments between dial-in users and other units on the CWAN and SIPRNET. This service could use a SMTP/POP/MS EXCHANGE server requiring a compatible e-mail client. The coalition web site could be hosted on web servers in the CAOC. To facilitate browsing by all forces, the web site would be replicated from SIPRNET web servers to Coalition web servers. Updates to the web site would be conducted as operational requirements dictate. Do to the use of https services, browser would require a current version of MS Internet Explorer V5.x or higher. The CWAN should support the exchange of classified files between all units utilizing an FTP server. These files would not be accessible to SIPRNET users, but could be transferred from the CWAN to SIPRNET and vice versa by trained staff system administrators. Web clients are acceptable programs for accessing the FTP services. CWAN policies would insure all e-mail messages transmitted from the classified SIPRNET to the classified CWAN and vice versa contain no attachments. Only e-mail with information classified releasable to Coalition users should be transmitted. Generally the producers of information are responsible for reviewing and approving the release of e-mail information prior to transmission. All data, services, and other controlled resources should be protected from unauthorized use. Users should have access only to data, services, and resources for which they have the clearance, authorization, need-to-know, and need-to-use. All users should be identified and authenticated before the users are granted access to data, services, and resources.

Intelligence Distribution

The CAOC Director of Intelligence is responsible for all intelligence operations in support of coalition ATO/ACO preparation and execution, including support for all intelligence organizations within the CAOC framework and at subordinate tactical units.

Responsibilities could include intelligence exploitation, fusion, and targeting operations. Additionally, they could also include the dissemination of intelligence information to the Coalition Air Component Commander staff, combat operation cell; combat plans cell; and subordinate tactical units to produce one commonly understood picture of the battlespace.

One of the major functions of intelligence is to maintain and distribute the current Order of Battle. Most likely in any theater the Commander-in-Chief (CINC) will be responsible for maintaining General Military Intelligence (GMI) information within his area of responsibility (AOR). The CINC will maintain this information in an MIDB server. The CINC organization could provide the same MIDB files to other key command control systems in the AOR. The CINC could also establish a dedicated GCCS-I^3 ISD server to provide the data extract to CAOC systems like TBMCS. Any operational or tactical unit could receive updates directly from this site. The CAOC should maintain a current tactical threat Order of Battle to support campaign planning and mission execution.

A secondary function of CAOC Intelligence is imagery storage and analysis. Imagery can be categorized into two basic formats: National Image Type Format (NITF), which is the future standard; and what may be referred to as a common workstation format (e.g., GIF, MIF, TIFF, and Sun Raster). The NITF format is complex and can contain multiple images, header data, symbol data, and unique data extensions.

One of technological ways that allows sensitive digital images to be tracked is to insert a covert digital watermark. The digital watermark would stay with that image, even as it is copied, altered and distributed. The digital watermark becomes an imperceptible part of that image, helping maintain an important link between the original image and any derivatives of that image. Watermarking will play an important role in enhancing the security of individual national states digital assets as they engage in daily CAOC functions.

Communications/Information Management

Coalition communication/ information management could include the following common functions as a minimum:

1. Track plain language addresses (PLA) and routing indicators (RI) to ensure message routing currency.
2. Ensure a common phone book is developed and distributed to all coalition members.
3. Coordinate fix actions on lost/delayed/misrouted message traffic.
4. Ensure a single distribution point for all incoming and outgoing messages. Direct alternate routing if a backlog develops.
5. Monitor ATO/ACO transmission to help ensure receipt and work with Combat Plans to resolve ATO transmission and receipt problems.
6. Build web pages and manage web information and shared folders.

Common Weather Picture

The CFACC will likely modify the presentation of the detail content of the weather briefing after the first few briefings. Generally the strategic or regional weather forecast will be on a less than SECRET LAN's web page along with a current satellite picture that covers the area of the AOR. Collocated with the web pages should be the official Horizontal Weather Depiction (HWD) forecast and other HWDs from other regional or strategic forecast centers. Based on the HWDs and the official Terminal Aerodrome Forecast for the next 24 hours, information about Coalition Airfield Weather, tactical locations weather, coalition weather forecasts out through 48-72 hours could be produced. High Frequency and Ultra High Frequency space weather information could be used to predict the Communication Impacts Due To Space Environment. Products that could be shared include:

1. Current Hemispheric or Global Meteorological Satellite (METSAT)
2. Current Regional or High Resolution METSAT
3. 0-24hr Cloud Cover And Weather
4. 24-48hr Cloud Cover And Weather
5. Coalition Airfield Weather 00-48hr
6. Communication Impacts Due To Space Environment, as required.

Conclusion

In conclusion, a road map has been proposed to support coalition integration and interoperability of information systems within a U.S. run Coalition Aerospace Operations Center. It is aimed to be used by personnel to explore how Command and Control systems (One set of systems on a US secure network and one set of systems on a coalition LAN) could work during experimentation. Military members (both US and Coalition), Contractors, acquisition, developmental test organizations, operational test agencies, and operational users are the key during C2 events and should document procedures and workarounds that improve overall CAOC system. This paper is not designed to provide standard operating procedures for any standing Coalition Aerospace Operations Center. Primarily, it is to provide operational users some insight into using more than one suite of equipment to prosecute a Coalition Air Operation.

This paper expresses in both operational and technical language the theoretical underpinnings required for experimentation to improve a notional Coalition Aerospace Operations Center.

References:

1. Jon L. Boyes and Stephen J. Andriole, eds., *Principles of Command and Control*, Foreword by Gen. Russell E. Dougherty (Fairfax, VA: AFCEA International Press, 1987).
2. Eric M. Grose and Mark W. Smith, “From Military Command and Control to Bond Trading: The Human Factors Process,” in *Proceedings of the Human Factors Society 36th Annual Meeting, SYSTEM DEVELOPMENT: Extending Military Human Factors* 2 (1992).
3. Melissa A. Cook, *Hewlett-Packard Company. Building Enterprise Information Architectures, Reengineering Information Systems* (Upper Saddle River, NJ: Prentice Hall PTR, 1996).

MARVIN L. “LENARD” SIMPSON, Jr. has a BS in Mechanical Engineering Technology from Virginia Tech University and an MS in Administration from Central Michigan University. He is now a Defense Contractor (L3 Com., Analytics Corporation) engaged in direct support to the Air Force Command and Control, Intelligence, Reconnaissance, and Surveillance Center led by Major General Robert F. Behler, after having completed 20 years as a member of the United States Air Force. His operational background includes experience in air-to-air and air-to-ground fighter missions, including the use of “special weapons,” leading operational support teams, exercise planning, and over 9 years in command and control informational systems. He is a recognized expert in the use of the U.S. Air Force’s Theater Battle Management Core System (TBMCS) and is familiar with most currently fielded Command and Control equipment. His technical skills include UNIX System administration, MCSE (CORE plus TCP/IP and Exchange), and PKI. He is a Commercial Pilot with more than 1450 flight hours in, F-4, T-43, T-37, T-38 aircraft and in general aviation aircraft.