Coalition Interoperability

A Pragmatic C4ISR Approach From The US Army CECOM Security Assistance Perspective

April 2003

William E. Skidmore, Sr.
MITRE
Washington C3 Center
McLean, Virginia
skidmore@mitre.org

Daniel Klingenburg
US Army Communications & Electronics Command (CECOM)
Security Assistance Management Directorate
Ft. Monmouth, New Jersey
daniel.klingenburg@us.army.mil

Abstract

Achieving coalition interoperability is difficult; competing National interests (military, economic or political) probably will necessitate imposing compromise solutions. Architecting solutions, which all respective parties would adopt and adhere to, is therefore problematic.

To address these problem areas, a combination of a system architecture and design methodology is employed that emphasizes the use of COTS products. There are several recognizable phases within this approach, most of which are recognizable:

- Operational capability requirement definition
- Analysis
- Architecture synthesis
- Component solution identification and capabilities assessment
- Design synthesis

This paper will discuss some of the problems defining interoperable coalition system architectures for these defined organizations and our approach to circumventing these obstacles. The paper will be presented from the US Army CECOM Security Assistance perspective in utilizing US grant funds such as Foreign Military Financing (FMF) to provide solutions for foreign militaries and multinational military organizations.

Section 1

Background

Achieving coalition interoperability is difficult; competing National interests (military, economic or political) probably will necessitate imposing compromise solutions. Architecting solutions, which all respective parties would adopt and adhere to, is therefore problematic.

Many formal and ad hoc coalition organizations have been formed in recent years to support peacekeeping and peace-support operations. The UN has deployed numerous of the former during its existence. Most recently, the military alliances have deployed multinational peacekeeping or peace-support organizations (e.g., SEEBRIG, SHIRBRIG, and BaltBat, etc.). Many nations have been provisioning selected units with advanced C4ISR capabilities just so that they can participate and interoperate in peacekeeping operations. Many of the members of these multinational organizations have never interoperated with some or all of the other organization members, and so the ability to interoperate in a C4ISR environment is largely an unknown. To address and moderate some of these issues, the US European Command (for example) has hosted an annual exercise (Combined Endeavor) to promote C4 interoperability for a number of years. Unfortunately, exercises such as these are not prevalent, and the alternative – a year-round interoperability testing and certification environment within the Area of Responsibility or alliance domain, is not on the horizon.

Currently, those military-focused C4ISR architecture modeling methodologies employed (when used) are often based on either the US DoD's C4ISR Framework or the NATO Policy for C3 Interoperability (as cited in the NATO C3 Technical Architecture (NC3TA)). Often, in many of the former Soviet-bloc nations, informal methodologies, utilizing vendor resources, are used. Typical are architecture studies that are done for Ministries of Defense, by defense contractors, at the recommendation of the same defense contractors, which heavily recommend those contractor's products.

Section 2

Interoperability Problem Space

Operational

Doctrinal and ad hoc operational interoperability are recurring requirements for military, peacekeeping and peace-support organizations. Essentially the same interoperability requirements extend throughout the vertical organization – from team, to brigade and division levels. Yet any form of doctrinal and ad hoc interoperability is dependent on a minimal infrastructure capability (e.g., communications), and the requirements should be defined as a product of interoperability exercises. Unfortunately, the lack of requirement documentation as a product of these exercises is the rule in most nations. Even where the requirements are captured, there is seldom any codification on expressing the requirement; this often results in confusion. The bottom line is that no one knows who has to interoperate with who or how.

Communications

Communications interoperability extends beyond different groups being able to communicate with each other. Within communications, even if the same standards are applied, there is no certainty that the implementation is the same. Even if the implementation is reused (e.g., COTS, GOTS), there is still no guarantee that the configuration of the implementation is the same. Year-round communications interoperability testing and certification is required; the closest thing to this is the Combined Endeavor exercise, hosted annually by US European Command (EUCOM). Even Combined Endeavor requires a series of planning conferences to assure each nation understands standards implementation and configuration, and how the exercise will be conducted, to insure that nations' representatives will be able to communicate with each other. There is no venue that exercises ad hoc communications interoperability. The conclusion, then, is that ad hoc communications interoperability is, at least, a bit of a misconception.

Communications security interoperability has been one of the most elusive, recurring issues facing nations' forces and planning staffs. No nation likes the thought of potentially sharing the keys to its intelligence – at best, they're afraid of the loss of control over the information. The logistics associated with common security techniques is staggering as well. The interim approach has been generally to invest in a coalition environment, where information is shared amongst participants using agreed to communications security procedures. The problem with this is that often the environment's classification level is at the greatest common denominator – this means that crucial information often is not shared because it cannot be downgraded to the appropriate level, or if it can, its utility will have expired. NATO has been trying to address this problem for years, and has yet to identify a satisfactory solution for all members.

Information

Information interoperability – now there's an interesting concept. If I say I have 50 gallons of fuel for my tank, my company commander would know what I mean; but would others? I mean, would they know that I was talking about diesel or aircraft fuel? What would be the grade of the fuel? How long could my tank run on 50 gallons; and under what conditions?

Generally, it extends to more than just being able to read data. Practically, it also applies to the ability to use the same data in multiple, different systems, and interpret it consistently across all systems. In practical terms, it could mean that consumption rates are calculated the same and the results not only look the same but also mean the same; everyone uses the same map symbol set and the symbol notations are in the same place in different systems and mean the same thing (nuances embedded in Mil-Std-2525b in part include differences in organization operational concept – like the difference between the US Army saying it has airborne infantry, and the an Eastern European country saying they have airborne reconnaissance forces - *although the they have no organic airborne delivery capability*); or that imagery can be utilized across systems. Message standards specify what categories of data go into each field, the size of each field, and the format of each field. They generally do not specify how the information is interpreted and used by different systems. Multilateral agreements (even informal ones), even within a nation's service, are often necessary to insure information interoperability and consistency.

Expanding Interoperability Gap

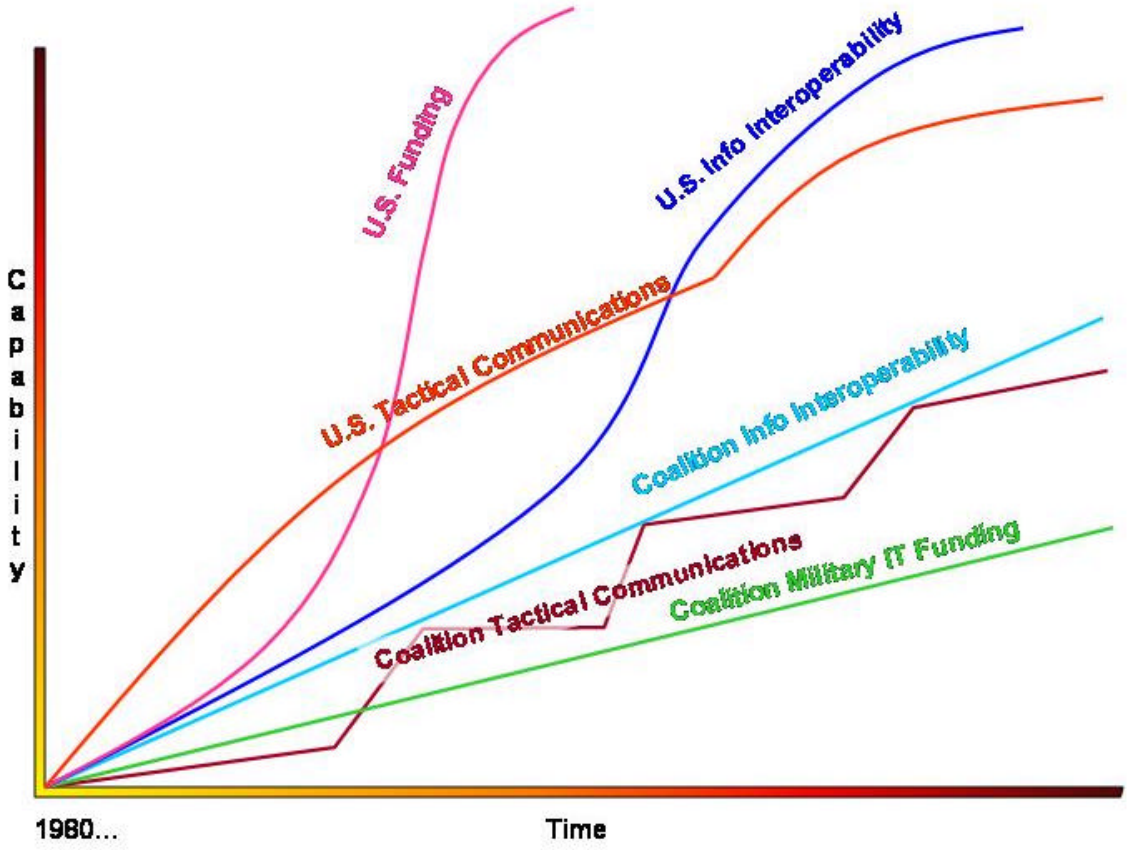
The following chart attempts to capture what many consider a critical problem for the U.S. and its allies over the next few decades – the widening capability gap.

This growing gap in capabilities is a direct result of increased US military funding during the latter stages of the Cold War and the efforts of the US Military to offset the perceived numerical superiority of the Warsaw Pact nations, primarily through the directed application of Information Technology (IT). When the Warsaw Pact disintegrated, the US really didn't slow the efforts to maximize effective use of Information Technology; there was no real "Peace Benefit" realized in the IT realm. Although military budgets were reduced, military investment in information technologies increased inversely to the reductions and often disproportionately so; for some period reflecting double-digit budget growth.

Our allies and former adversaries, on the other hand, were dealing with drastically reduced military budgets fueled by the popular view that since there were no threats and enemies, there really wasn't much need for a military force, coupled with shortsighted resource allocation of what they had had. Large military bureaucracies had to be supported; there was no room to dedicate funds to new military planning and operations automated command and control systems, or to upgrade existing combat systems with new technology. In other words, transformation was not a priority.

The following chart relates the US funding of the 1980's to the explosion in US military capabilities seen in the 1990s and during operations Enduring Freedom and Iraqi Freedom, in relation to the capabilities of our coalition members.

US tactical communications experiences surges in capabilities, largely because the upgrades mandate huge reinvestments in capital expenses. Because these investments in any given



technology cannot be done continuously (imagine replacing all of the SINCGARS radios every year!), significant gains in performance and interoperability happen sporadically and over long periods. Information processing, on the other hand, has tended to adopt a more robust version of spiral engineering, whereby the software systems are in constant development with (relatively) frequent upgrade deployment. The rapid growth in information interoperability can be considered a symptom of the nearly concurrent and horizontal acceptance and incorporation of information technology across the breadth of the US arsenal, coupled with the warfighters' understanding of the practical application of the technologies and the benefits of joint interoperability driving additional requirements (solution) development. This has in part been driven by the Joint Readiness Training Center (JRTC) facilities and the subsequent development

of corresponding codified joint doctrine. The knee in that curve is a result of the anticipated overall slowdown in gains in interoperability as the easy solutions are implemented and the more difficult issues (which require more detail to understand and time to solve) are addressed (given a constant level-of-effort).

Comparatively, the improvement of the interoperability capabilities of our coalition partners has been slower to realize. National mandates for support of improved interoperability, inferred by military funding as a percent of GDP, has been significantly less than what even NATO considers necessary to achieve a critical mass (NATO guidelines for Nations military funding are currently pegged at 2% of GDP). In many of the more advanced, industrialized coalition partners, military funding is considerably below the 2% threshold, and is largely used for pay and allowances, both of the military personnel and the civil (i.e., unionized) servants that support them. In those nations with significantly reduced military funding over a long period, there are precious few (if any) resources remaining to support interoperability transformation.

In those nations that utilize US Foreign Military Financing (FMF) grant funding, improvements can reflect a "stepped" escalation in capability, specifically associated with funding levels, prioritization of requirements, and technology insertion. Many of our new coalition partners do not have the national budget to be able to purchase or develop (on their own) the interoperability capabilities needed to keep in step with the US's evolutionary transformation, and therefore rely heavily on the US FMF year-to-year funding. Because of the year-to-year vagaries of FMF funding amounts, coupled with changing urgencies of competing requirements, comprehensive solutions, even over a long term, are seldom implemented – limited FMF funding and changing national priorities do not support that kind of approach. Interoperability improvement in many of our coalition partners therefore devolves into band-aid application – fixing only as much now as is needed to solve immediate problems, hoping that the situation will improve at a later time to enable a more aggressive overhaul. This then is reflected by the "stepped" curve – a herky-jerky approach to modernization.

Despite this kind of approach to modernization, coalition partners' information interoperability has been seen to improve at a more consistent pace – no large capital expenses are generally required, AND they take full advantage of lessons learned to enable them to maximize the efficiency of their efforts. In short, they don't have to make the same mistakes we did, and therefore are better able to target specific work on addressing their information interoperability problems.

Despite the positive efforts of coalition partners, parity with current US military technology will never be attained at the current funding levels – we're still funding at a greater level, and we are continually refining systems, based on feedback on operational and prototype systems.

Section 3

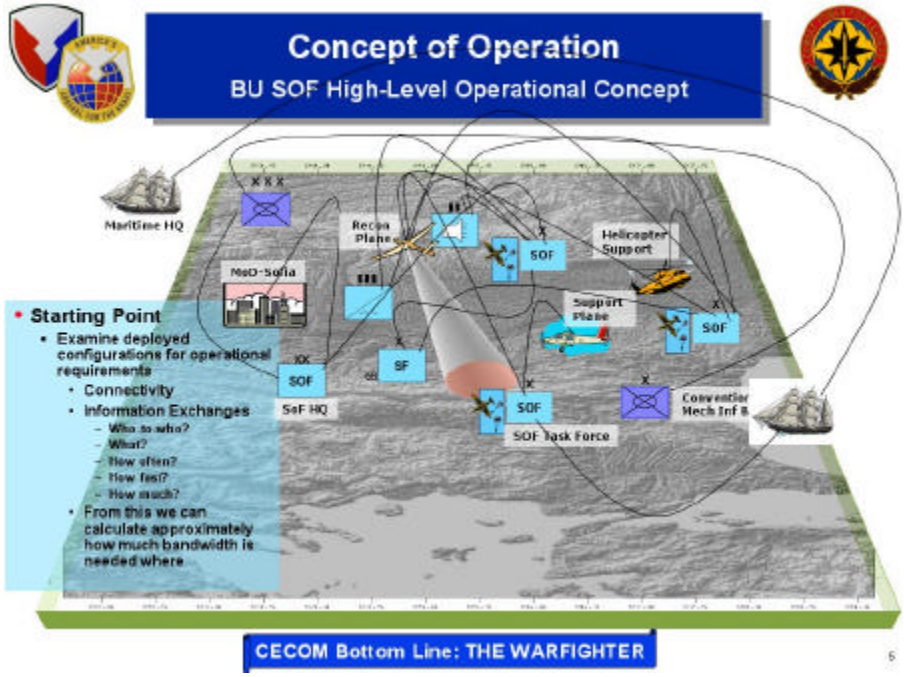
Circumvention and Nullification Approaches

To address these problem areas, we utilize a combination of a system architecture and design methodology that emphasizes the use of COTS products. Predominantly based on the US DoD's C4ISR Framework, but incorporating aspects of various software and systems analysis processes, it provides sufficient detail to enable a Nation to make informed decisions on what-to-obtain-when to achieve internal interoperability, as well as interoperability with identified nations, governmental organizations, and non-government organizations. There are several phases within this approach, most of which are recognizable from various systems analysis processes:

- Operational capability requirement definition
- Analysis
- Architecture synthesis
- Component solution identification and capabilities assessment
- Design synthesis

Operational Capability Requirement Definition

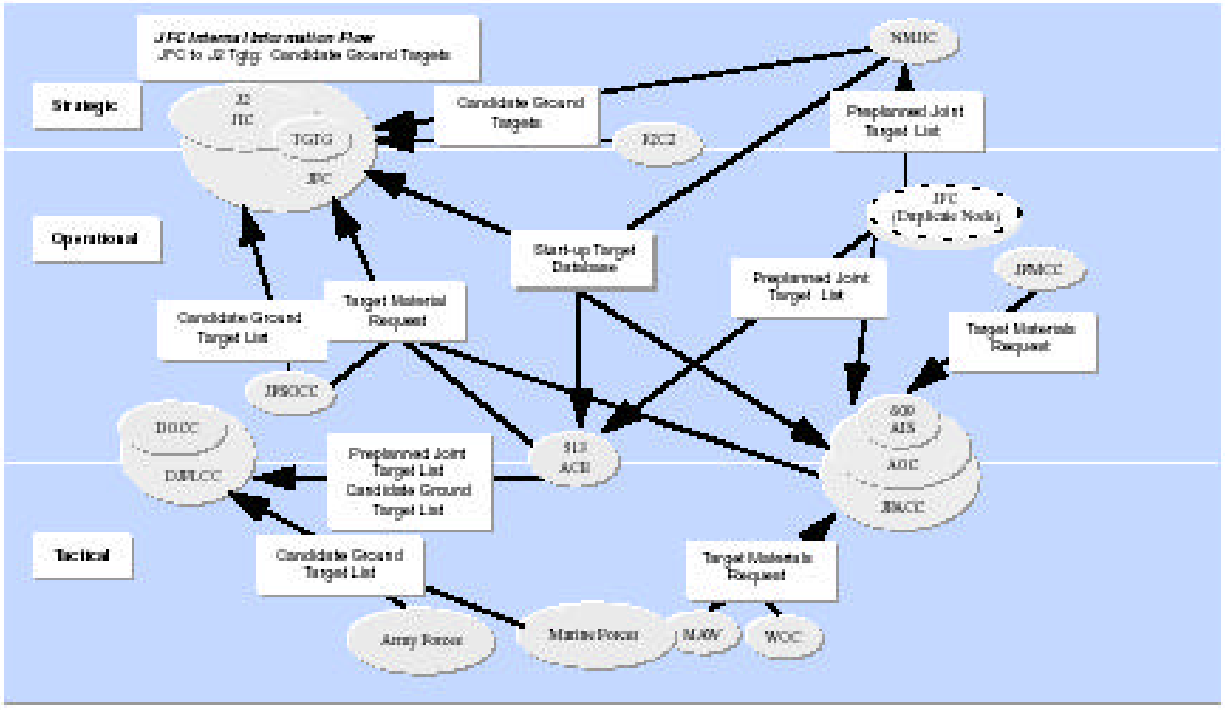
In the C4ISR Framework, this can be distilled into three primary products:



- High-level operational overview (see above example) - the most general of the architecture-description products and the most flexible in format. Its main utility is as a

facilitator of human communication, and it is intended for presentation to high-level decision makers.

- Operational Node Connectivity - features of this product are the operational nodes and elements, the needlines between them, and the characteristics of the information



exchanged. Each information exchange is represented by an arrow (indicating the direction of information flow), which is may be annotated to describe the characteristics of the data or information (e.g., its substantive content, media [voice, imagery, text and message format, etc.]), volume requirements, security or classification level, timeliness, and requirements for information system.

- Operational Information Exchange Matrix – Information Exchange Requirements

Operational Information Element (Name/Identifier)	Description	Media	Size	Units	Operational Element and Activity				Frequency/ Timeliness/ Throughput	Security	Interoperability Requirements
					Producer Identifier	Producer Activity	Consumer Identity	Consumer Activity			
FPLT/Fwd HQs											
OPORD	Operations Order	Paper	12	MB	SEEBRIG HQ	G3	FPLT/FWD HQ	Commander	As Necessary	U	ADATP3
FRAGO	Alert Notice	Message	100	KB	SEEBRIG HQ	G3	FPLT/FWD HQ	Commander	As Necessary	U	ADATP3
SITREP	Situation Report	Message	80	KB	FPLT/FWD HQ	Commander	SEEBRIG HQ	G2/3	Daily	U	ADATP3
Map	Mission Maps	CD or Paper	50	MB	SEEBRIG HQ	G3	FPLT/FWD HQ	Commander	As Necessary	U	ADRG (?)
Pictures	Pictures	CD or Paper	30	MB	FPLT/FWD HQ	Commander	SEEBRIG HQ	G3	As Necessary	U	JPEG, TIFF
MCP											
OPORD	Operations Order	Message	18	MB	MCP	COMSEEBRIG	Nations	Commander	As Necessary	U	ADATP3
FRAGO	Alert Notice	Message	100	KB	MCP	COMSEEBRIG	Nations	Commander	As Necessary	U	ADATP3
SITREP	Situation Report	Message	80	KB	MCP	COMSEEBRIG	Higer Cmd	Commander	Daily	U	ADATP3

identify who exchanges what information with whom, why the information is necessary, and in what manner.

Our initial efforts utilize these procedures to document any requirements based on existing capability, and to project the operational and system impacts of any anticipated or desired capability improvement or expansion. In many instances in dealing with foreign militaries, information inter-relationships and the derived resultant loading of the infrastructures has never

been captured, projected, or analyzed. In some instances, the inter-relationships are not well understood. Walking the Client through the operational concept and information exchanges helps to clarify the desired versus expected performance environment of the CIS system, as well as insuring that the Customer fully comprehends the operational scope, interdependencies, and constraints of the capability they are attempting to procure.

Requirement Analysis

Incorporating the data associated with the information exchanges, as well as proto-views of functions, portals, etc., the specific CIS functional and operational requirements are defined. In many instances, this would include country-unique capabilities based on established or developing doctrine, as well as requirements derived from cultural, economic, or political sensitivities. Graphical examples of requirements become critical, as it helps clarify any language and technical disparities. Supporting text is also a critical requirement for this process, as often briefings are not retained or do not translate well. By compiling briefings into position or whitepapers, it allows the clients to properly translate and consider findings absent of the pressure of translating on-the-fly AND understanding the technical material.

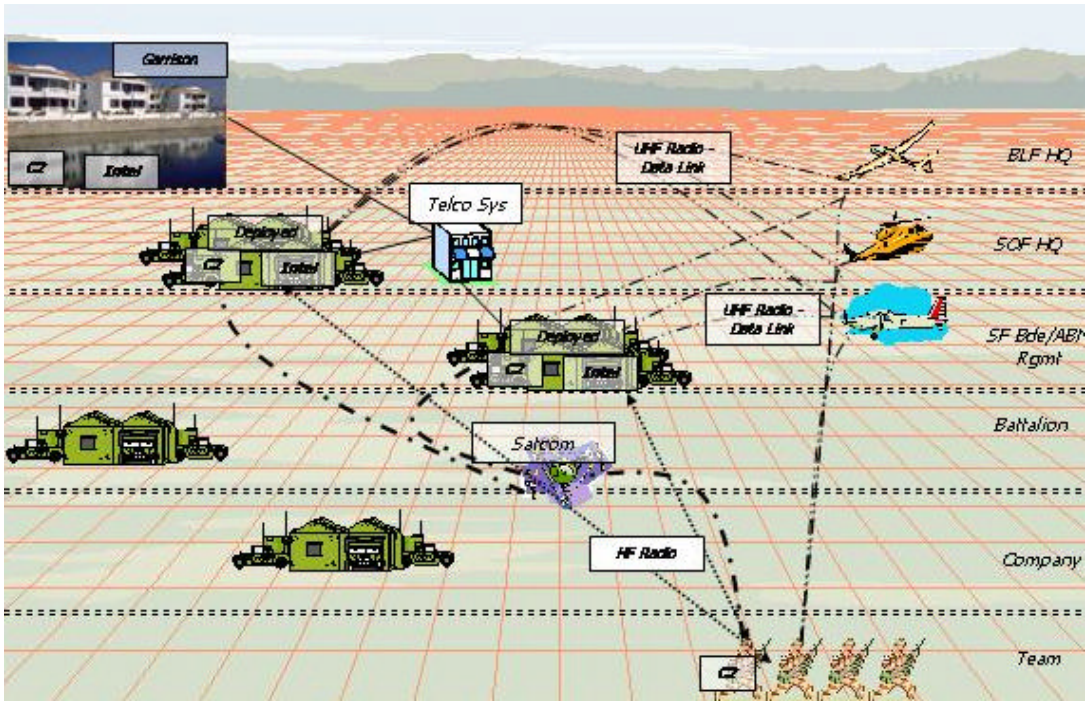
Usually, once the character of the information exchanges are considered, additional, derived requirements begin to surface. Requirements analysis, itself, is a spiral process, interacting with the synthesis of the architecture to evolve, clarify, and decompose requirements to the requisite level so that they are associated with specific components, as well as pointedly involving the Customer to promote clarification and understanding.

Architecture Synthesis

Technology Assignment

Based upon the operational requirements (e.g., distance, performance, survivability), critical infrastructure technologies are allocated between top-level nodes (see diagram on next page). Communication with the Customer is critical during this stage, as Customer "buy-in" to the architecture AND solution is paramount to minimize miscommunications. Nothing can be more frustrating to all concerned than delivery of a system architecture or solution, and there is disagreement on what was understood would be provided.

Another consideration is technology's costs. Many coalition members cannot afford their own satellite services due to relatively high recurring service costs; the conventional means of



long-distance, mobile, wireless communication for them is High Frequency (HF) radios. Unless, as a matter of policy, the coalition command organization or host organization is willing to provide satellite or other similar wireless support, they should only be considered as "future objective" components of the architecture; near-term, cost-conscience capabilities must be provisioned in the architecture to insure interoperability upon initial implementation. (Need to make the distinction between coalition operations and multinational organizations such as SEEBRIG. I don't think folks will understand the statement "parent host Nation's organization)

Usually, there is an operational requirement for telephonic communication; three complimentary approaches are evolving.

- The standard is conventional military telephone communication. Support for analog phone and inter-switch trunks, as well as Radio Telephone Integration (RTI), were standard services. New twists include digital telephone instruments that provide the user with an LCD display (e.g., CallerID and other advanced services), and fully digital switches that support a multitude of services, including Ethernet switching and routing, RTI, analog services, and ISDN and EUROCOMM standard trunking interfaces.

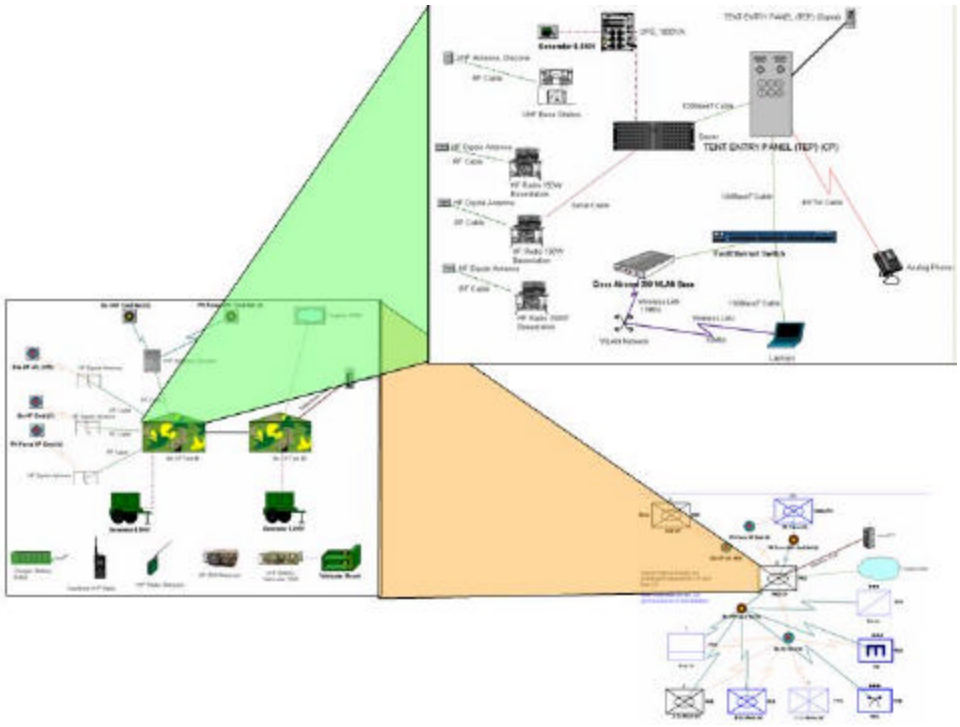
- TETRA (Terrestrial Trunked Radio) is a set of standards developed by the European Telecommunications Standardization Institute (ETSI) that describes a common mobile radio communications infrastructure throughout Europe. This infrastructure is targeted primarily at the mobile radio needs of public safety groups (such as police and fire departments), utility companies, and other enterprises that provide voice and data communications services. TETRA actually takes its features from several different technological areas: mobile radio, digital cellular telephone, paging, and wireless data.

TETRA-based products come with built-in encryption features to ensure the privacy and confidentiality of sensitive data/voice communications. These products are also designed with the ability to transfer data at faster rates than seen before in mobile communications. These features make it very attractive for some military applications, including peacekeeping and peace-support operations (see http://www.commcomms.co.uk/dindex.htm for features of the Dolphin ExpressNet service). The downside to this system is the inherent significant cost of the infrastructure if not previously installed.

- Voice-over-IP (VoIP) is a leading edge technology that transmits voice IP packets over the local and wide area networks. The technology is transparent to the users; there is specialized routers, call managers, and telephone sets that must be used. The real shortcoming is the lack of standard interfaces into the overseas PTTs or other Nations' or coalition's equipment, specifically some of the ISDN implementations and the EUROCOMM interface specifications. Unless the calls are routed through an intermediary service that can support the router's interfaces for VoIP as well as the interface to the local PTT or military organization, VoIP devolves into a closed system.

Optimized Process

We find that usually, the top-down analysis approach described in the C4ISR Framework works very well in decomposing functional entities into specific capabilities or components, and lends itself to simpler and more concise explanations when reviewing architectures with clients.



The diagram above shows how we utilize the Framework's decomposition process with relatively inexpensive software tools to achieve a completely interoperable solution architecture. In this case, components are allocated to specific requirements until each requirement is fully

addressed. This requires a full understanding of both the requirement's implications (explicit and inferred), as well as appropriate characteristics of hardware and software components.

Software elements are especially difficult to characterize within the Nation's system architecture, because the time allocated for the study is constrained, and/or the interrelationships between C2 applications and software subsystems are characteristically complex. While architecting a communications infrastructure is initially a straightforward proposition which is solely based on the operational requirements, refinements and performance upgrades are often needed when the software inter-process communications are factored in. This is especially true when employing simpler technologies. The most stereotypical communications changes involve an initial architecture dependent on HF communications for long-distance, wireless communications.

HF communications, in the era of gigabit data rates, has been characterized as the poor-nations answer to satellite communications. Except for the capital costs, it is free – no recurring service fees are attached to its use. The downside, in this age of force digitization, is the extremely limited data transmission capabilities, which, despite the occasional hype from HF radio vendors, is usually characterized for planning purposes as 2400 bps. When a client says that they want to be able to transfer a multi-megabyte file between two points, with a speed-of-service requirement of 20 minutes, AND they want to rely on HF radios for the transmission, explaining why that cannot be done to clients that have never transmitted data in a tactical internet, and then recommending alternative approaches to accomplishing the same function, can become laborious.

Depending on the funding profile for the efforts, we may recommend developing an architecture for a functional slice (e.g., field artillery) of the military forces in lieu of a broad, but limited depth, analysis. Performing a functional slice analysis has real value and enables the analyst to develop an evolution roadmap in sufficient detail to adequately support clients' business decisions.

Identifying the 60+% Solution

Many times Nations will request more in US grant funds than what their FMF funding profile can support. We have habitually made recommendations on how to scope the effort to fit within their current profile, or to spread the effort over multiple years so that they can attain the complete solution that they desire.

Requirement prioritization becomes extremely important to all concerned. Arbitrarily specifying the operational priorities could lead to deliver of a system that, while it meets the requirements specified in the contract (i.e., Letter of Offer & Agreement in Security Assistance speak), the delivered system may not satisfy the urgent operational requirements of the Users.

It has been historically difficult to get Nations to prioritize their system requirements, especially when it would mean some requirements (often those politically attractive) would only be addressed in the out-years, if at all. Nation's Ministries of Defense and their staffs have to make often painful (and sometimes potentially career-ending) decisions. In many of the former Soviet states and Soviet-allies, requirement prioritization is a relatively new thing to them.

So, to get to the 60% solution, requirements are prioritized and allocated across a timeline (multi-year, if necessary), and adequate funding is identified and dedicated, to insure that the highest-priority requirements (and the derived requirements needed to support the high-priority ones) have sufficient funding to produce a solution. Once there is a partial solution available and in the hands of the Users, follow-on funding is easier to obtain to address the balance of the requirements. This is slightly different than the generally accepted way of doing spiral engineering and development, but where funds are severely constrained, the answer is to strategize the solution.

References:

NATO C3 Technical Architecture (NC3TA), ADatP-34, http://194.7.79.15/, version 4.0 (7 March 2003), ISSC NATO Open Systems Working Group

C4ISR Architecture Framework, v2.0, 18 December 1997, The Architectures Directorate of the C4I Integration Support Activity (CISA), Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (OASD[C3I])

Security Assistance Management Manual, DD5105.38, www.dsca.mil/samm 5 February 2002, Defense Security Cooperation Agency

Doctrine for Joint Special Operations. Joint Pub 3-05, 17 April 1998, US Joint Staff

European Telecommunications Standards Institute (ETSI), www.etsi.org

NATO: U.S. Assistance to the Partnership for Peace (20-JUL-01, GAO-01-734), United States General Accounting Office.