Determining Communication Shortfalls for Homeland Defense

Strategic Insights, Volume VI, Issue 6 (December 2007)

by MAJ Kevin P. Wilson

Abstract

Communications is a critical enabling capability that is interwoven into every facet of every military operation. Assessing what communication capability is most valuable to the operation is a vital planning requirement that currently resides in several processes that produce differing outcomes within the DoD. This article examines these planning processes, particularly the capability-based approach, assessing which process is optimal for determining communication shortfalls.

An in-depth comparison of the Joint Capabilities Integrated Defense System (JCIDS) and USNORTHCOM's Capability Review and Resource Assessment (CRRA) was conducted, examining the respective strengths and weakness of each process. This article then recommends an optimized hybrid solution of the CRRA and JCIDS, thus providing an intuitive methodology that can be used to model what communication capabilities are essential to the DoD and its interagency partners.

Ultimately, this model may serve to guide the defense planning process to ensure meaningful collaboration occurs, when crafting a unified DoD and interagency position regarding communications and network-centric capability needs and shortfalls. Particular utility can be applied to fill the gap of interoperable communications solutions between first responders, the military, interagency, and coalition partners, when teaming in a homeland defense scenario.

Introduction

A major shift is occurring within the DoD regarding the development and funding of communication requirements for the services. Transformation from the Cold War, coupled with the events of 9/11, has forced the DoD to change its rules of engagement when it prioritizes and funds communications systems for the warfighter. Aging platforms and the war in Iraq have further increased competition for funding among the services, thus complicating the decision-making process for senior military leaders.

During the height of the Cold War, when pockets were deep and the adversary was a symmetrical actor, funding decisions were reached using the BOGSAT (Bunch of Guys Sitting at the Table) method.[1] This method was an exercise in service parochialism steeped in emotion and politics, where the highest ranking or most protected leader prevailed. Over time, the

BOGSAT system evolved into a more qualitative approach, where requirements were validated by linking mission impact to the perspective communication system. However, this approach still lacked the quantitative rigor necessary to ascertain an objective analysis.

In June of 2003, the DoD issued CJCSI 3170.01, Joint Capabilities Integration and Development System (JSIDS), with the intent to migrate from a platform-centric procurement process to a capability-centric approach.[2] This approach employs a series of Joint Functional Concepts (JFCs) to identify critical capabilities that deliver a desired effect to the combatant commander. In the communications arena, the Network-Centric Environment (NCE) JFC is utilized to capture communication shortfalls for the DoD. The Air Force[3] and Navy[4] have since followed suit by developing their own service-centric Capability-Based Planning (CBP) process to identify communication shortfalls.

This article examines current methodologies used in the DoD to ascertain communication and network-centric capability shortfalls for warfighters and first responders. The objective is to develop an intuitive and meaningful methodology that defense planners and programmers can adopt to discern communication shortfalls, quantify and articulate those shortfalls, and then, in turn, use that data to help decision-makers prioritize funds when procuring systems that provide communication capabilities for Homeland Defense. The key research question analyzed is: Does CBP possess the right methodology to assist defense planners and programmers in determining capability gaps/shortfalls?

There is no text book to assist planners on the art of CBP methodology or processes. DoD instructions describe a capability assessment used by Combatant Commands, known as Joint Capabilities Integration and Development System. Currently, several methodologies exist in the DoD and each one differs in their application and execution. Each directorate of the Joint Staff employs its own unique Joint Functional Concept. Nearly every concept discusses communications, but each concept differs in articulating and quantifying what a capability is and how to measure its effectiveness.[5]

This research is intended to provide alternative methods for Combatant Commands, primarily USNORTHCOM, to plan and fund communication capabilities for Homeland Defense. U.S. Joint Forces Command may also find value in this process and use it as a template across the DoD and Joint Staff.

Further, this article will stress the importance of collaboration among the COCOM, Joint Staff, and services when planning, staffing and executing the Program Objective Memorandum (POM) during and between Future Years Defense Program (FYDP). This is a critical element of defense planning since precious resources are often wasted as the result of poor collaboration and non-standard processes occurring simultaneously which fail to capture a unified DoD position when articulating capability needs and shortfalls.

Communication Shortfalls: Background and Framework

The world is now at the height of an information revolution where the dissemination and analysis of data is critical to government, commerce, and world culture. From a national defense perspective, communications is an enabling capability that is interwoven into every facet of military operations. The term “communications” is often interchanged with concepts such as the Network-Centric Environment and C4 (Command, Control, Communications, and Computers).[6] This is mainly due to the evolvement of electronic technology with the advancement of electrical component miniaturization, as well as that of computers, computer software, and its Internet-worked architectures.

During World War II and through the Cold War, the term communications represented a category of technology such as radio, radar, telephone, telegraph, and teletype. By the 1960s, satellite communications were introduced to the DoD[7], which provided an optimized voice or telephony[8] capability to the warfighter, and ushered in space-based communication technology.

Am Important step occurred in 1969, when the University of California at Los Angeles (UCLA) installed the first Advanced Research Projects Agency (ARPA) node,[9] sharing digital packet information with the Stanford Research Institute, the University of California at Santa Barbara (UCSB), and the University of Utah.[10] This birth of the Internet further shaped military communications as it merged traditional communications, such as radio, video, and telephony services, with computer technology. This synergy became known as network-centric, as these services can now be integrated and transported over networks and shared with multiple users.

The Network-Centric Environment is defined as “a framework for full human and technical connectivity and interoperability that allows all DoD users and mission partners to share the information they need, when they need it, in a form they can understand and act on with confidence, and protects information from those who should not have it.”[11]

Several of these terms require further definition. First, the concept technical connectivity implies equipment or hardware that is connected or interconnected together. Second, interoperability can be defined as "[t]he ability of systems, units or forces to provide services to and accept services from other systems, units or forces and to use the services so exchanged to enable them to operate effectively together.”[12] Third, information is defined as "[f]acts, data, or instructions in any medium or form with context that is comprehensible to the user.”[13] Finally, “all DoD users and mission partners” refer to all branches of the services working with interagency partners, such as the intelligence community, the Department of Homeland Defense, the State Department, the Department of Justice, etc. Needless to say, many of the challenges in the communications area, from a DoD perspective, arise from the dramatic recent expansion of who its “mission partners” might be under given circumstances, and the need to develop systems that can take account of their requirements in a timely manner.

Simply put, communications, C4, the network-centric environment, or net-centricity, might be best understood in the context of homeland defense as connectivity and interoperability that allows all DOD users and mission partners including Joint, Coalition, and Inter-Agency users to share information when they need it, in a form they can understand and act on with confidence, and which also protects information from those who should not have it.

It is important to examine the components, or functions, that make up the repository of communications or net-centricity. Three categories provide a valuable framework for this discussion.[14] They are: voice, video, and data. The following definitions depict these categories:

- Voice—Provide information via [human or computerized] voice to include: radio, phone, interphone, voice-over IP, or public address system.[15] Or, the frequency of an acoustic oscillation which may be produced by the normal human voice.[16] For further clarity, interphone is defined as: A telephone apparatus by means of which personnel can talk to each other within an aircraft, tank, ship or activity.[17] Voice systems are typically found in radios that reside in aircraft, ships, ground vehicles, and portable backpacks versions.
- Video—Information such as: streaming video, video teleconferencing, live transmissions, or recorded video.[18] Video is the images captured by camera and displayed via various types of displays such as: a computer, television, cell phone, multi-function displays in aircraft, ships, our ground vehicles. In a collaborative

setting, video is captured via a web camera or cellular phone and shared over the internet or cellular network as raw data or during chat sessions.

- Data—Text or imagery such as: digitized photos, forms/publications, email, messages, Web pages, chat sessions, or audio files.[19] This data is created by manual input such as a keyboard, stylus, digital camera, or scanner. The data is disseminated manually by humans or automatically by machine, network, or Internet processes.

How Are Communications Applied to Homeland Defense?

Communications applied to the defense arena, specifically to homeland defense, become more complex and advanced. In addition to enabling C4 functions, communications enable space, intelligence, surveillance, and reconnaissance (ISR) functions.[20] Space and C4ISR platforms are extremely network-centric. They are a system of systems interconnected via networks to collect, process, and disseminate data. Further, Space and C4ISR platforms typically integrate the three categories of communication capability, namely: voice, video, and data. For example, a Defense System Communication Satellite III is capable of sending voice, video, and data worldwide to a variety of military and government users. The satellite itself orbits in space at an altitude of 22,000 miles, but is controlled by a series of ground stations that are interconnected by network-centric technology. Users on the ground, at sea, or in the air can access this system to receive and disseminate data to conduct operations.[21]

In addition to disseminating data, imagery and infrared sensors reside on defense satellites providing valuable ISR for homeland defense. Infrared sensors on the Defense Support Program Satellite provide early warning detection of missile launches against the United States or personnel operating overseas. Again, this is a high orbiting satellite that is controlled by ground stations that are interconnected by network-centric capability and the information is processed, analyzed, and disseminated by similar technology.[22]

The next important facet of these capabilities is the integration of these various sensors, signals, and raw data. What is critical for the DoD and its interagency partners is the sharing of these systems to make intelligible decisions. This is often called decision-quality information derived from sensor integration or decision superiority.[23] The newly published Joint Operating Concept for Homeland Defense and Civil Support provides an excellent explanation of this concept, discussed in the Battlespace Awareness section of the document:

“Battlespace awareness is the ability of the Joint Force Commander to understand the operational environment, the full array of interagency and international capabilities, and the adversary. To ensure DoD can detect, deter, prevent, or if necessary defeat threats to the Homeland and assist in mitigating the effects of attacks that do occur, the Joint Force Commander must have a comprehensive understanding of the battlespace (within the limits set by law). This includes the capability to detect the full range of threats enabled through an interlocking field of sensors with deep reach and remote surveillance capability, fused with national-level intelligence collection and analysis to provide common situational awareness across the spectrum of participants for all domains in the operating environment (air, space, land, maritime, and cyber). For HD and CS, this includes shared awareness (including non-intelligence sources) between numerous government and non-government participants.”[24]

In addition to the interlocking or integrating a field of sensors and the fusing of national level intelligence discussed here, an underpinning of information sharing is essential to decision or information superiority. This implies technical solutions, as well as a profound alteration of the culture of sharing information that has traditionally existed within the intelligence community, the DoD, and its likely coalition or interagency partners. This is perhaps the most difficult barrier to

overcome since it involves the human element of how operations are conducted. This can be overcome by fostering a spirit of openness and sharing. This concept is described in the net-centric JFC as end-to-end transparency. This is a concept of opening up technical and cultural barriers, thus providing information to those who need it and is defined as: visible, accessible, understandable, verifiable, current, and trusted.[25]

A final important communication concept applied to homeland defense is the advent of wireless technology. Wireless solutions provide homeland defense personnel with a portable, lightweight, and secure capability that allows for the collection, analysis, and dissemination of information.[26] This is an important aspect since these personnel may deploy, in an austere or a ravaged environment where fixed infrastructure is not available or has been damaged by an attack or natural disaster. This technology provides an agility factor for personnel who must deploy with little or no notice and have limited space and weight allowances to transport large amounts of equipment and personnel to operate it.

A few of these devices may include: personal digital assistants (PDAs), cellular telephones, laptop or knee board computers, handheld radios, global positioning service receivers, and a myriad of wireless sensors to collect and disseminate vital imagery, weather, and chemical, biological, radiological, nuclear, and explosive (CBRNE) data.

Wireless technology provides interconnectivity from the sensor to the decider to the shooter and or responder. It provides a push pull collaborative ability between these entities, facilitating centralized decision-making with decentralized execution. An effective wireless solution has the ability to integrate the three components of communications, voice, video, and data, in a seamless manner to those individuals who require and are authorized access to the information.

An area of technology that is bringing wireless technology to fruition is the development and fielding of unmanned aerial vehicles (UAVs). UAVs are able to collect various ISR information, such as: voice, video, data, weather, radar, and CBRNE, and disseminate it back to distributed ground systems for processing and analysis. This information can then be pushed or pulled to various personnel who may need it to conduct homeland defense missions in virtually any environment, in the air, on land or sea, or from space.

What Is a Shortfall and Why Is it Important?

Before shortfalls can be discussed, it is essential to understand what a capability is. Capabilities are often confused with systems, platforms, tasks, or effects. The joint staff defines capability as: “The ability to execute a specified course of action. It is defined by an operational user and expressed in broad operational terms in the format of an initial capabilities document or a DOTMLPF change recommendation. In the case of material proposals, the definition will progressively evolve to DOTMLPF performance attributes identified in the CDD and the CPD.”[27]

Though a system or platform delivers capability and provides effects, it is not a capability in itself. Computer networks and handheld radios are systems or solutions, not capabilities. They provide capabilities such as, wireless voice and data services to the operator, but are not capabilities by themselves.

Nor should capabilities be confused with tasks. Regarding communications and NCE capabilities, the capability may be: provide voice communications on the ground, air, or sea, and not install VHF radios, antennas, and cabling in ground facilities. The capability is the what, not the how or why. Capabilities are produced by systems and platforms and contribute the desired effect, but are not stand-alone systems, platforms, or effects.

As capability has been defined, shortfalls and gaps must be understood. In the capabilities planning arena, gaps and shortfalls are used interchangeably. The joint community explains capability gap(s) as: “The capabilities are identified by analyzing what is required across all functional areas to accomplish the mission. The gaps or redundancies are then identified by comparing the capability needs to the capabilities provided by existing or planned systems.”[28] The inability to provide those needs results in a capability gap or shortfall.

This often tedious process requires that available integrated architectures be analyzed and compared to the combatant commands Integrated Priority Listing. The IPL is the operational requirement stated by the combatant command and is often non-descriptive. The challenge is matching these non-descriptive requirements to existing or future systems that may or not provide the needed capability. Another challenge to be mindful of is that integrated architectures are not systems, but “[a]n architecture consisting of multiple views or perspectives (operational view, systems view and technical standards view) that facilitates integration and promotes interoperability across capabilities and among related integrated architectures.”[29] What planners must do during this process is to establish the linkages between architectures and systems.

In the context of NCE, information support plans aid the process by establishing these linkages by describing “system dependencies and interface requirements in sufficient detail to enable testing and verification of information technology (IT) and National Security Systems (NSS) interoperability and supportability requirements. The ISP shall also include IT and NSS systems interface descriptions, infrastructure and support requirements, standards profiles, measures of performance and interoperability shortfalls.”[30] This is important, because NCE is an enabling capability that underpins all military operations. Therefore, system dependencies, interface requirements, and interoperability must be in constant consideration.

What is the importance of communication gap analysis? Aside from merely heightening everyone’s awareness that communications are the enabling capability of most military/civil operations, its real utility comes from how it affects the decision-maker who allocates funds. The catch phrase often heard at the Pentagon by senior officers and executives is: “If I had one more dollar to spend, where should it go?” Gap analysis helps answer this question by inserting several decision points into the acquisition process that forces the decision-maker to assess how capability gaps are maturing and where to direct resources to close these gaps. If the maturity process is going poorly, flag officers and senior executive may decide to stop funding to a particular program and divert funds where more progress is being made.

If the shortfall is validated correctly, in the context of meticulous capability-based planning, a common thread or traceability may be established throughout a myriad of operations. For example, if it is determined that a data shortfall has been identified and it is occurring across several joint capability areas[31], such as land, sea, space, and defense support of civil authority operations; this implies the criticality of this particular shortfall. This provides decision-makers an integrated analysis to consider what is more rigorous and objective than traditional procurement processes. This provides combatant commanders’ shortfalls to present that have been validated in a joint environment across several types of operations, thus lending to the credibility of the funding decision.

Defense Planning: Connecting the Dots

America’s Defense Strategy

The *National Defense Strategy of the United States of America* is the Department of Defense’s plan to align its objective against America’s grand strategy. Published in March 2005, it was better aligned with the White House’s *National Security Strategy* of September 2002.

Nonetheless, similarities reside in the two documents and the Pentagon has made the connection in the strategic objectives, implementation guidelines, and in the desired capabilities and attributes section of the document.

Primarily, America's defense strategy speaks of building on the *2001 Quadrennial Defense Review* by implementing transformation via a capabilities approach. Four strategic objectives have been established which link fairly well to the grand strategy. They are: "secure the United States from direct attack; secure strategic access and retain global freedom of action; strengthen alliances and partnerships and establish favorable security conditions."[32] These four objectives would require the same type of enabling communication capability as were linked to America's National Security Strategy, namely voice, video, and data used in the air, land, sea, and space domains. Further, the same attributes would also apply, such as: interoperability and multi-level security. Multi-level security speaks to information sharing amongst mission partners who have a need to know. These partners may exist as: foreign governments/coalition partners; interagency partners; federal, state, local, and tribal governments; and joint military organizations.

As stated in this strategy:

"Capabilities-based planning focuses more on how adversaries may challenge us than on whom those adversaries might be or where we might face them. It focuses the Department on the growing range of capabilities and methods we must possess to contend with an uncertain future. It recognizes the limits of intelligence and the impossibility of predicting complex events with precision. Our planning aims to link capabilities to joint operating concepts across a broad range of scenarios."[33]

It can be argued that this is one of the key elements used to transform the military, shifting focus from a threat-based planning model to the capability-based model.

This document goes on to introduce the Defense Department's desired capabilities and attributes. There are eight of them:[34]

1. Strengthen Intelligence
2. Protecting Critical Bases of Operation
3. Operating from the Global Commons
4. Protecting and Sustaining Forces in Distance Anti-Access Environments
5. Denying Enemies Sanctuary
6. Conducting Network-Centric Operations
7. Improving Proficiency Against Irregular Challenges
8. Increase Capabilities of Partner-International and Domestic

This is where this document begins to unravel. These eight items do not meet the criteria of defined capabilities per the guidance from the Joints Chiefs of Staff. Per their guidance, the J7 has identified and grouped operational capabilities into tiers, thus prioritizing and establishing a common language amongst the joint community. For example, the J7 has a few of the following as core capability areas:[35]

- Joint Land Operations
- Joint Maritime/Littoral Operations
- Joint Air Operations
- Joint Space Operations
- Joint Access & Access Denial Operations

- Joint Information Operations

The difference between the two lists is apparent. The first is a list of objectives or tasks, whereas the latter are distinct capability areas employed by the military. Hence, this is where the confusion begins in the planning and programming communities. It incites the community to lean back towards their comfort zone and think in terms of requirements, task, systems, and platforms.

The other document that is responsible for defining national defense strategy is the *National Military Strategy of the United States of America*. This document is intended to bridge the gap between the White House and the SECDEF strategies. Signed in 2004 by former Chairman of the Joint Chiefs of Staff, General Richard B. Myers, it focuses on capabilities and attributes. They are:[36]

- Applying Force
- Deploying and Sustaining Military Capabilities
- Securing Battlespace
- Achieving Decision Superiority

Like the National Defense Strategy, these four capabilities do not meet the criteria as defined by the J7 as capability areas. Again, these four items are more objectives or tasks. Another problem with the defense strategy is how attributes are defined. In the National Defense Strategy of 2005, two attributes are identified: shape and size of military forces and global defense posture.[37] These are not attributes, because they cannot be measured. However, in the National Military Strategy, the following joint force attributes are listed:[38]

- Fully Integrated
- Expeditionary
- Networked
- Decentralized
- Adaptable
- Decision superiority
- Lethality

These attributes are more readily measurable, often associated with a unit of measure such as a percentage. Therefore, work remains to refine these documents to establish a common language in the planning community.

USNORTHCOM'S Defense Strategy

The next linkage that requires analysis is how USNORTHCOM implements grand and defense strategy. NORTHCOM's strategy is derived from the December 1, 2006 document titled, *Strategic Guidance, Defending Our Homeland*. Though this document does not mention America's security, defense, or military strategies, a linkage can be found in the dilation of its strategic goals and objectives. The intent of this document is to "provide strategic direction to ensure unity of effort within and between NORAD and USNORTHCOM."[39]

NORAD and NORTHCOM are collocated at Peterson Air Force Base in Colorado Springs, Colorado, staffed with over 1,400 Army, Navy, Air Force, Marine Corps, Coast Guard, civilian and Canadian personnel. These two commands have complementary missions to secure the North America. The following mission statements depict these complementary roles:

NORAD Mission Statement

- Detect, validate, characterize, assess, and warn of attacks against North America whether by aircraft, missiles or space vehicles. Detect and respond to unauthorized and unwanted air activity approaching or operating within North American airspace. Process, assess and disseminate intelligence/information to warn of maritime threats or attacks against North America.[40]

USNORTHCOM Mission Statement

- Conduct operations to deter, prevent, and defeat threats and aggression aimed at the United States, its territories and interests within the assigned area of responsibility; and as directed by the President or Secretary of Defense, provide defense support of civil authorities including consequence management operations.[41]

Simply, NORAD's responsibilities remained unchanged prior to 9/11 whereas NORTHCOM was established to handle the interagency and military/civil relations issue.

These complementary roles can be further articulated and the nuances detected in the two commands by the following strategic goals:

NORAD's Strategic Goals[42]

- Detect, deter, and defend against aerospace threats to North America
- Provide timely, accurate maritime warning of threats to, and attacks against North America
- Be a model for international cooperation in defense planning, execution, training, information management, and technological innovation

USNORTHCOM's Strategic Goals[43]

- Detect, deter, prevent, and defeat external threats and aggression
- Provide timely and effective defense support of civil authorities
- Improve unity of effort with our interagency and international partners

Combined Strategic Goal

- Create a more agile organization that takes care of its people and meets the challenges of the 21st Century[44]

Though this organization appears redundant, it is solidified by one commander, who is dual-hatted to lead both commands, a similar model to what was used when USSPACECOM and NORAD were led by one four-star flag officer from the 1980s through 2002. In October 2002, USSPACECOM was disbanded, with the Space and C4ISR roles transferred to USSTRATCOM.

This is not to say that NORAD and USNORTHCOM have relegated all Space and C4ISR oversight to USSTRATCOM. On the contrary, the very nature of securing America via NORAD and NORTHCOM is completely reliant on Space and C4ISR capabilities. In reality, what is

occurring is a division of labor to divvy up this tremendous workload associated with planning, programming, and executing the types of capabilities and assets required to support the above strategic objectives.

Further dilation of NORAD's/NORTHCOM strategic guidance is derived from NORTHCOM's *Concept of Operation Plan (CONPLAN) 2501-05*. This 555 page CONPLAN, published in April 2006, was created to fulfill the following requirement: "USNORTHCOM CONPLAN 2501-05 fulfills a requirement established in the Joint Strategic Capabilities Plan (JSCP) 02 Change 1, Regional Tasking 9. The CDRUSNORTHCOM was directed to prepare a plan to support the employment of DOD forces providing Defense Support of Civil Authorities (DSCA) IAW applicable DOD directives and policy."[45]

This plan was crafted to help bridge the gap from strategic guidance to actionable tasks of securing the homeland. It contains ten annexes which call out specific actions to meet the commander's intent. Of the ten annexes, seven invoke communications or NCE capabilities. The following table links some of the more critical communication/NCE capabilities to the applicable annex:

Table 1: CONPLAN2502-05 Communications Requirements

Annex	Communications/NCE Requirement
A – Task Organization	National Imagery Collection and Analysis
B – Intelligence	Interagency Data Sharing (CIA/NSA/DIA)
C – Operations	Common Operating Picture Generation
K – C4	Satellite Communications/Wireless
Q – Health Services	CBRNE Detection and Processing

What is significant about this table is that it can act as a point of origin for the methodology of the CBP process, particularly when developing models to capture shortfalls.

Discerning Needs: The BOGSAT

The BOGSAT, a Bunch of Guys Sitting Around the Table, method is evolving towards a more quantitative method. Though efforts have occurred to change this paradigm, namely by instituting threat-based planning during the Cold War period and introducing CBP post-Cold War, the BOGSAT paradigm is hard to kill. It continues to emerge in most corners of government, including the DoD, especially pertaining to areas of homeland defense.

A book authored by Ernest Forman, Professor of Management Science at George Washington University, discusses the pitfalls of the BOGSAT process. Here he iterates that the BOGSAT is the most frequently-used decision method in use today. Further he states:

"Even though there may be considerable preparation for a BOGSAT, including information-gathering, and detailed analyses (e.g., financial, marketing, technical, political, etc.), there are numerous problems with this approach. According to Peter Beck, 'These sessions are often dominated by the leader and rarely facilitated. The leader sets the tone and is often not challenged. If the group starts down the wrong path they rarely look back.'…However, times are changing and many organizations have been abandoning the BOGSAT in favor of more capable methods."[46]

Forman continues to reveal the central problem of the BOGSAT as the cognitive limitations of the human brain. Competent decision-making requires following these subsequent steps:[47]

1. Perfectly defining the problem
2. Knowing all relevant information
3. Identifying all criteria
4. Accurately weighting all the criteria according to his/her goals.
5. Accurately accessing each alternative on each criterion.
6. Accurately calculating and choosing the alternative with the highest value

Also, the BOGSAT require the following to be relevant process: “A BOGSAT discussion typically involves dozens of ‘things’, e.g., issues, alternatives, pros, cons, objectives, criteria, etc.”[48] Simply, most humans are not trained and/or conditioned to follow this mental checklist to ensure their decision-making is sound. When the decision process grows too complex or stressful, humans will default to using their gut instincts or migrate toward the comfort zone of their emotional biases. Often, as a built-in coping mechanism, humans will attempt to simplify or de-scope the problem in order to comprehend it or find a low hanging fruit solution to rectify the problem. This is problematic as this simplifying or de-scoping often indeed changes the nature of the problem itself. Therefore, when a solution is offered, it is the wrong solution for the wrong problem.

Another issue that is related to this phenomenon is a term called "thin slicing." Thin slicing is a method to make decisions quickly in times of crisis. Thin slicing is a technique that resides in the military and first-responder culture, where fireman, police, and soldiers, will make split second decisions based on a sixth sense which is developed after years of exposure to life threatening situations where certain sounds, smells, or images prompt a person to decide or act quickly to save lives or thwart disaster.[49] Though this is a crucial skill for first responders, it could prove disastrous in the defense planning sector, as procuring capabilities requires methodical and careful planning where programs are funded over three, five year defense programs.

What is ironic about the defense culture is that the key decision-makers concerning capability procurement are flag officers who are typically force application operators who have developed the thin slicing technique in combat and major combat operations over years of military service. This would imply that these decision-makers might be predisposed to thin slicing and come to the table ready to make split or gut reactions without following a methodology or type of model.

Perhaps this is why there is such opposition to defense planning processes that are steeped in rigor, such as CBP. It is a process that is foreign to the tactical culture. Though flag officers have years of strategic and operational experience, their formative years were spent at the tactical level, relying on their gut and acting quickly in times of stress and crisis.

With regards to defense planning at USNORTHCOM, CBP has been adopted, but not fully embraced. In addition to JCIDS, NORTHCOM has developed a process called the Capabilities Review and Resource Assessment (CRRA). This is not to be associated with the CRRA used by the Air Force, which is the Capability Risk and Review Assessment. NORTHCOM’s CRRA is conducted by J81 and is consistent with the JCIDS process. Though NORTHCOM is working to institute their version of the CRAA, capability decisions are still sometimes conducted using the BOGSAT method. This is not a problem unique to NORTHCOM. CBP is a new discipline within the DoD and will take years to modify a culture that cut its teeth on Cold War programmatics.

The same problems that perpetuate the BOGSAT at the senior decision-making level is also felt at the action officer level of many staffs. Unlike the flag officer, who has had years of operational and strategic level exposure, the action officer may have little, if any, strategic experience. They come from the tactical arena where decisions are made quickly and they bring with them thin slicing skills that are razor sharp. This is also true for Program Element Managers (PEMs). PEMs think in terms of platforms and systems, not capabilities. Moreover, PEMs live in a culture where

defending platforms occurs at all costs. The outcome of their fitness reports is directly proportional to the survival of their responsible system, not by the desired effect their systems provides to the combatant commander.

Another irony that exists on many staffs is that the director was once a PEM when he or she was a new field grade officer reporting to their first assignment at the Pentagon or Joint Staff. This makes for an interesting dynamic as staffs have essentially evolved, or are evolving, in a PEM culture. This is where the double-edged sword emerges. Services must defend programs that are directly tied to their portion of the total obligation(al) authority of the defense budget, while justifying the necessity of these programs that should be tied to its capability which, in-turn, produces a desired effect.

JCIDS

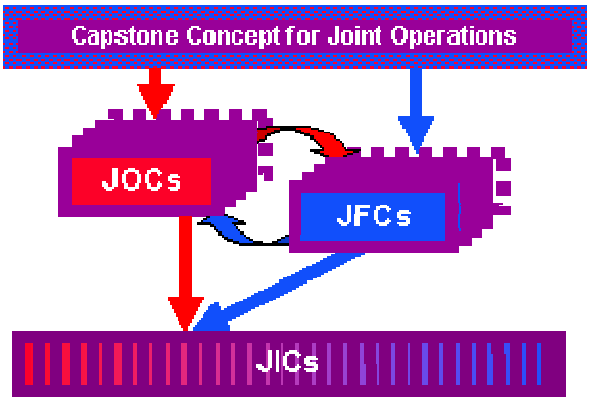
JCIDS is the current model used by the DoD to capture capabilities strengths and gaps to help shape funding decisions for a wide variety disciplines or focus areas, such as: force protection, battlespace awareness, force application, focused logistics, command and control, and the network-centric environment. These disciplines are encapsulated by what is known as a family of Joint Operations Concepts. The following statement captures the intent of this design: “In April 2003, the Secretary of Defense directed the development of the Joint Operations Concepts (JOpsC) family. This family consists of a Capstone Concept for Joint Operations (CCJO), Joint Operating Concepts (JOCs), Joint Functional Concepts (JFCs), and Joint Integrating Concepts (JICs). These concepts look beyond the FYDP out to 20 years.”[50]

Each concept has its place in the CBP process and each concept is published in corresponding documents. The following definitions and figure help delineate this family of documents:

- CCJO—“Overarching concept of the JOpsC family that guides development of future joint force capabilities. Broadly describes how the joint force is expected to operate in the mid to far term, reflects enduring national interests derived from strategic guidance, and identifies the key characteristics of the Future Joint Force.”[51]
- JOC—“Operational-level descriptions of how a Joint Force Commander will accomplish a strategic mission through the conduct of operational-level military operations within a campaign. Applies the CCJO solution and joint force characteristics to a more specific military problem. Identifies challenges, key ideas for solving those challenges, effects to be generated to achieve objectives, essential capabilities likely needed to achieve objectives and the relevant conditions in which the capabilities must be applied.”[52]
- JFC—“Describes how the Future Joint Force will perform a particular military function across the full ROMO. JFCs apply the CCJO solution and joint force characteristics to the specific military problem. They identify the required functional capabilities needed to generate the effects identified in JOCs and identify attributes needed to functionally support the Future Joint Force. JFCs address Tier 1 Level Joint Capability Areas.”[53]
- JIC—“Describe how a Joint Force Commander will perform his operations or functions that are a subset of JOC and JFC capabilities. JICs address Tier 2 Level or below Joint Capability Areas. JICs have the narrowest focus of all Joint Future Concepts and describe capabilities and decompose them into task level detail. An illustrative vignette is applied to the JIC to describe the environment in which

these tasks will be performed. The standard of performance for these tasks is described in a common taxonomy for concepts and capabilities."[54]

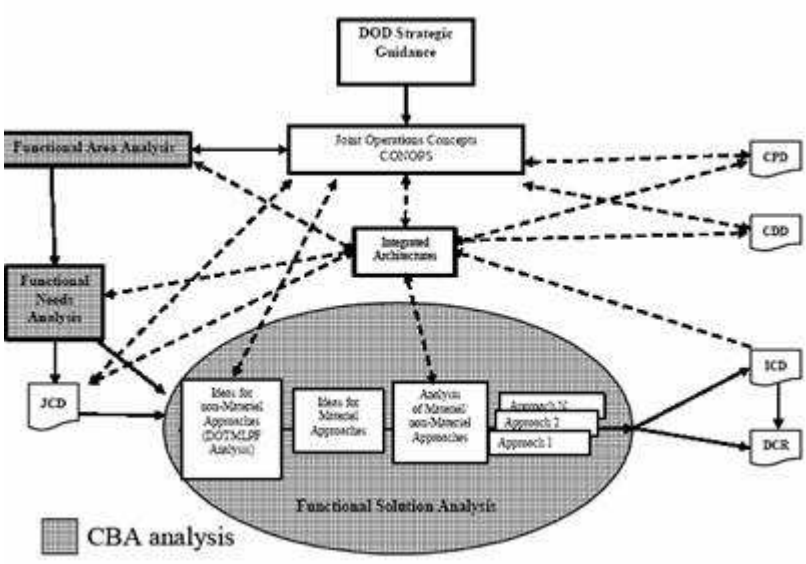
Figure 1: JOpsC Family[55]



This family of documents thus becomes the reference materials for Capability-Based Assessments (CBA) within the JCIDS process. First it is important to understand what the CBA is. CJCSI 3170.01F, states: "The CBA is the JCIDS analysis process that includes three phases: the FAA [functional area analysis], the FNA [functional needs analysis], and the FSA [functional solutions analysis]."[56]

The FAA defines the military problem, scopes the problem, introduces capabilities needed, and links those capabilities to defense strategy. The FNA is the portion of the CBA that begins to discern gaps in capabilities. Here capabilities are scored using the context of the scenario in the FAA. The FSA, as the name implies, is the process which recommends solutions to capability gaps ascertained in the FNA. These solutions are often broad and overarching, identifying both material and non-materials solutions to rectify the gaps.

Figure 2: The JCIDS Analysis Process[57]



Therefore, for the purposes of this article, analysis of the Net-Centric Environment JFC and JIC will be conducted as the JFC and JIC contain the specified parameters to conduct the CBA such, as: the scenario or vignette and the capabilities and attributes to be scored during the assessment to determine gaps or excess. The following figure helps visualize this complex process:

Identifying Communication Shortfalls for USNORTHCOM: Current Methodology

NORTHCOM has adopted a derivative of JCIDS called the CRAA. This CRRA is not be confused with the Air Force CRRA, but is essentially JCIDS coupled with an Interagency Coordination (IC) component to facilitate their mission of providing defense support for civil authorities. This IC component allows collaboration with interagency partners which, in turn, provides input for their CRRA process.

The CRRA is conducted annually by the J5 and J8, with J8 acting as office of primary responsibility for the overall codification process. The CRRA work in concert with the planning, programming, budgeting, and execution cycle, to support NORAD and NORTHCOM's commitment to fulfill national military strategy. This methodology is used to help identify current and future capabilities and help guide the command's investment decisions. The output of this process is presented to the Office of Secretary of Defense, other defense agencies, the Joint Staff, the services, and to the Canadian department of National Defense to inform this community on capability development, acquisition, sustainment, and investment needs.[58]

Guidance for the CRRA process is contained in NORAD/USNORTHCOM Instruction 90-144 and is compliant with the following DoD and Joint instructions/processes:

- CJCS Instruction 3170.01E, JCIDS
- CJCS Instruction 6212.01D, Interoperability and Supportability of Information Technology and National Security Systems
- DoD Directive 5000.1, the Defense Acquisition System
- DoD Instruction 5000.2, Operation of the Defense Acquisition System
- DoD Directive 7045.7, Implementation of the Planning, Programming, Budgeting System

As the CRRA is a new process, it is more of a vision than a reality. This is the first time the CRRA has been conducted and, as with any new concept, it is just beginning to make traction. NORTHCOM is the newest combatant command and is barely getting its arms around JCIDS, let alone its recent cousin, the CRRA. Though it offers promise, particularly regarding its interagency collaboration piece, it will have to survive cultural barriers and the plethora of taskings that seem to plague higher headquarters organizations.

As for determining communications shortfalls for homeland defense, the J6 has yet to adopt the CRRA. Currently, they are utilizing the JCIDS process, primarily focusing on the NCE JFC and JIC as the instruments to conduct their analysis. Though this directorate is valiant in pursuing this process, the NCE JFC and JIC are laden with their own unique set of problems which impede the NCE planning process in the context of homeland defense and security.

This leads to the most important aspect of capability-based planning: the context in which one discerns capability gaps. The context is based on the scenario that is at the front end of the model. This is the lens that helps the planners and subject matter experts determine what environment they are to operate within. In the case of JCIDS or NORTHCOM's CRRA, this

scenario is contained in the JFC. The scenario contained in the NCE JFC is a vignette occurring in Turkey, involving the capital city which is struck by an 8.2 magnitude earthquake, displacing thousands of Turkish citizens and destroying or disrupting Turkey's critical infrastructure.[59] While this type of vignette is likely to occur, much like how Hurricane Katrina transpired, it is only a single event. Though it is an adequate starting point, NORTHCOM will surely be faced with multiple events that will exceed the intensity of a natural disaster.

More appropriately, the NCE JFC should contain a series of events that would reside in NORTHCOM's purview. More precisely, multiple events in the homeland and abroad are more realistic. Events such as a dirty bomb detonation in the port of Long Beach, followed by a Tsunami in Australia, topped off by a string of IEDs in downtown Manhattan during rush hour. The diversity and intensity of these simultaneous events would provide the adequate stress in the model to keep SMEs and planners attentive.

Strengths and Weaknesses of Current Processes

A key weakness is now identified that begins to clear the path for what is right and what is wrong with NORTHCOM's model. Starting with its strengths was the fact that the J8 Directorate realized JCIDS was a not one-size-fits-all model. Their initiative to establish the CRRA is evidence that the command is serious about solving interagency NCE shortfalls. Establishing the IC component of the CRRA is a very pragmatic solution to enable collaboration with non-DoD partners. While this is often a painful pursuit of clashing cultures, it will pay dividends when capturing the right expertise and perspectives when pinned together during reoccurring forums. Eventually, these forums will condition themselves to overcome these cultural barriers, ultimately developing the right network of planners to solve interoperability problems.[60]

Further, the CRRA provides NORTHCOM with a quantitative assessment of end-to-end look at capabilities, addressing desired effects. It attempts to link strategy to capabilities and then, to desired effects. This process is the catalyst to evolve from the BOGSAT which still resides at NORTHCOM and other higher headquarter institutions.[61]

While the J8 is working hard to institutionalize a capability-based model that works for the command, several weaknesses are inherent in the process. These weaknesses apply to both the JCIDS and CRRA models adopted by NORTHCOM. This implies that NORTHCOM is not solely in error, but that the Joint Staff has created a model that is too complex and labor intensive. In an effort to design an encompassing process, it is has become over engineered and far too difficult to comprehend. Too many working parts reside in the process and it requires months, if not years to master. Over 500 pages of esoteric guidance must be consumed before a participant is to gain an elementary working knowledge of the NCE portion of JCIDS.

Action officers assigned to labor in this discipline lack the continuity to gain in-depth expertise. Often, action officers change assignments several times within their tours, barely scratching the surface, then moving on to new duties. Even if the directorate is staffed with an action officer who can provide continuity, the SMEs tasked to provide the analysis have to be trained or retrained to perform their duties, often in a very narrow time slot. What exacerbates this problem further is the fact that few action officers are dedicated solely to the JCIDS or CRRA process. They are encumbered with multiple taskings unrelated to capability-based planning, that clouds their ability to focus and spend the adequate time necessary to develop the proper methodology and analysis to garner NCE gaps.

The same problems experienced by the action officers responsible to administer these processes also pertain to the SMEs who are tasked to perform the scoring and analysis of the JFCs and JICs. Few, if any, headquarters possess the sufficient number of SMEs organically to analyze the diversity and complexity of the NCE JFC and JIC. Thus, headquarters must solicit help

throughout the services to find the right mixture of expertise to conduct the appropriate level of analysis needed. Hence, the problems of over tasking and lack of continuity permeates into this body, where understanding and ample time to dedicate to the process is absent. This ultimately affects the control group used, as the base of action officers and SMEs are so dynamic that perceptions, expertise, and interest drive different scores and outcomes from year to year. Just finding and maintaining a usable repository of SME who are willing in able to participate in the planning process, is a full time responsibility.

In addition to personnel issues that affect the control group, the ability to quantify the criterion of the NCE standards and measures of the JIC is problematic. This criterion is too specific to be scored in any given scenario. For example, if response time to provide connection to U.S. and non-U.S. networks is the standard being measured and the criteria is 30 to 60 seconds, how can that be measured? Does someone have a stopwatch to monitor every connection in every work center? Of course not. Thus this criterion loses its utility and SMEs typically respond with something like, "it depends."[62]

Further, the amount of capabilities, tasks, and standards contained in the JIC are too great and require far too much time to analyze. Many of these can be eliminated to simplify and expedite the process. Most organizations lack the luxury for their action officers to dedicate this much effort in a supporting role.

An Optimized Proposal[63]

In an attempt to alleviate the problems associated with the JCIDS model, this article offers a more intuitive and simplified capability-based model. The model offered here is an overview of a hybrid of several planning models, not an all encompassing proposal, but contains sufficient detail to articulate its utility. For the purposes of this model the following critical elements must be covered: the Scenario, the Master Capabilities Library (MCL), SME Selection, and the Forum.

The Scenario

The scenario is the first lens to look through and the most important. The scenario is the event or events which provides context or sets the stage of the operation. It provides the who, what, when, where, and why of the operation. For example, if the military is engaged in operations with civil authorities, such as evacuation efforts due to natural disaster or a CBRNE event, the scenario helps provide the operational environment or situation in which personnel and equipment operate. This is critical as it helps planners visualize what stressors affect the operation.

For the intent of this model, it is important to select a scenario that is most stressing. This ensures planners select the right capabilities to be evaluated or applied to the event. The Office of Secretary of Defense (OSD) has been tasked to identify the most stressing scenarios to our nation and military. Two Major Conflict Operations (MCOs) are applied, plus four vignettes should be applied to the methodology.[64] Vignettes are CBRNE and natural disaster events and thus are perfectly matched for first-responder operations. Further, a CBRNE event would be the most stressing to civil authority and first-responder communication systems, as it is a worst case scenario which could occur to our country. Communications systems would have to be survivable to electro magnetic pulse, interoperable with military, federal, state, and local agencies. This does not imply that capabilities must be gold plated, but acts as a reminder of the severe environment present for planners and SME to keep in the back of their minds when conducting analysis. In order to facilitate this, a scripted briefing containing the details of the scenario and its vignettes must be crafted and presented to the entire body conducting the analysis at the initial stage of the process. Also, it should remain present during the duration of the planning session and be cited in the published findings of the analysis. This assists planners and SME from reverting to previous real world events or lessons learned which not the intent of this type of analysis.

The intent of this model is to capture current and future capability shortfalls for current plus two FYDPs, thus aligning itself with the POM of the services supporting NORTHCOM. If documented correctly, this provides extremely important justification to programmers to defend their systems that fill the shortfall gap. However, this must be validated by participants from the Joint Staff, NORHCOM, and the services.

The MCL

The MCL is a repository of capabilities, not tasks. The MCL consists of five distinct parts: the category, the domain, the capability, the attribute, and the Measure of Performance (MOP). It is the primary tools for SMEs to score the maturity of capabilities

The category, Provide the Network-Centric Environment, is a modified definition from the NCE JFC which is more applicable for HLD operations. It should read: Connectivity and interoperability that allows all DoD users and mission partners to include: Joint, Coalition, Inter-Agency, Federal, State, and Local First Responder users to share information when they need it in a form they can understand and act on it with confidence, and protects information from those who should not have it.

The domain is the environment personnel and equipment operates in, such as: land, sea, air, and space. The domains are defined in the following manner.

- Land—Operations where personnel and equipment reside on the ground, such as: search and rescue operations, police and fire operations, Command and Control (C2), Nuclear C2 (NC3), and Special Operations (SOF) missions.
- Sea—Operations where personnel and equipment reside on the water, ocean, lake, and river, such as: port security, search and rescue, counter sea operations, and NC3.
- Air—Operations where personnel and equipment reside in the air, such as: air strike, C2, Intelligence, Surveillance and Reconnaissance (ISR), and, NC3.
- Space—Provide services/connectivity to and from assets used in operations that occur in space, such as: space situational awareness, offensive counter space, defensive counter space, missile warning, surveillance, communications, precision navigation and timing, nuclear command and control, and weather.

As previously mentioned, the capability is what service is being delivered, not the system or the solution. Therefore NCE capabilities in its simplest form are: provide voice, video, or data services. Capabilities are defined in the following manner:

- Voice—Information, such as: radio, phone, interphone, voice over Internet Protocol, or public address system.
- Video—Information, such as: streaming video, video teleconferencing, live transmissions, or recorded video.
- Data—Information, such as: text or imagery, such as: digitized photos, forms, publications, email, messages, web pages, chat sessions, or audio files.

Attributes are the characteristics of the capability which gives it uniqueness or desired level of performance. These attributes are defined in the following manner:

- Timely—Expected timeliness to meet mission requirements. Implies latency, speed, and responsiveness of systems and information in all environments.
- Availability—Information access, anytime/anywhere. Implies adequate bandwidth, redundancy and self-healing/self-forming architecture. Includes Machine to Machine (M2M) interconnectivity.
- Survivable—Expected to survive in multi-environments: electro-magnetic pulse, directed energy attack, and radio frequency attack. Implies the capability is hardened to withstand physical attack.
- Low Probability of Intercept/Low Probability of Detect—Ability to provide low probability of intercept and detect. Implies ability to operate in anti-access environments where low observable and stealth are required towards mission success.
- Protected—Information is expected to withstand information attack or compromise from an adversary. Includes information assurance attributes, such as: authenticity and non-repudiation. Further implies multi-level security capabilities to appropriately share information with coalition, DoD, inter-agency, federal, state, and local partners.
- Useable—Ability to operate the system with little or no effort or training. Implies the system is intuitive to operate and the output is decision quality, discernable, and easy to comprehend. Further implies the appropriate human factor analysis has occurred to ensure ease of operation and comprehension of information flow.

The final component of the MCL is the MOP. The MOP is the value function that is scored by operators, planners, and technical experts to assess the respective capability and its attribute. The process consists of two parts: establishing the value function and assessing the capability and attribute. Establishing the value function is accomplished first. This is where the operator expresses the required level of performance and what attribute is essential for mission success. Then, NCE planners and Subject Matter Experts (SME) will assess and score to determine if existing capabilities meet the value function. If not, then a potential capability gap is discerned and recorded for further analysis and validation.

Four categories are assigned to the value function: No Military Value (NMV), Limited Military Value (LMV), Good Enough (GE), and More Doesn't Matter (MDM). The critical step is establishing the GE value, as GE is the goal to discerning if appropriate capability exists. Anything less implies a capability shortfall, while anything more implies excess and the capability does nothing more to enhance the mission. This is accomplished in a collaborative effort with planners and operators looking through the scenario lens and judging what capabilities are needed, what corresponding attribute is essential, and what MOP is necessary to accomplish the mission. The following table illustrates the useable attribute:

Table 2: Attribute and MOP Depiction

Useable	1. Unable: NMV: 1-10
Ability to operate the system with little or no effort or	2. Extreme Difficulty: NMV: 11-20
training. Implies the system is intuitive to operate and	3. Considerable difficulty: LMV 21-40
the output is decision quality, discernable, and easy to	4. With Some Effort: LMV: 41-79
comprehend. Further implies the appropriate human	***5. With Minimal Effort: GE: 80***
factor analysis has occurred to ensure ease of	
operation and comprehension of information flow.	6. Completely Intuitive: MDM: 81-100

For example, if an operator needed data services in the land domain, useable would be a relevant attribute. Now, at what level does useable become necessary to accomplish the mission? What threshold can the operator live with where more really does not matter to complete the mission? If completely intuitive provides no advantage over minimal effort, then the value function becomes 5—with minimal effort.

Once the value function has been set, now the planner and SME can assess to determine what systems and platforms provide this type of capability and perform at the level. If not, then a potential capability shortfall may exist.

To illustrate this collective process, consider if Monterey was responding to an earthquake. The earthquake would become the scenario or vignette and would contain certain stressors such as: no electrical power, buildings destroyed, fire, etc. The first responder or fireman would have to determine what communication/NCE capability is needed to accomplish their mission. They decide handheld radios are necessary and useable is a required attribute. They further determine that the GE value is 5, useable with minimal effort. Now the SME and planner can assess their current radios to determine if they meet that value. If not, a possible shortfall exists and then they begin the validation process to discern if shortfalls exist and begin to package the data in a decision quality format. Once the data is validated and formatted, planners present the data to decision-makers, who prioritize funding requirements for annual procurement budget decisions. This process provides an objective and quantitative approach.

SME Selection

Another critical element of this model is the selection of subject matter experts (SMEs). As described in the MCL portion of this article, the MOP is a two sided equation, analyzed by two types of SMEs. The operational SME is an expert well-versed in a particular operation contained in the scenario. For the purposes of the HLD vignette discussed earlier where Monterey suffered from an earthquake, fireman, police, and military assisting in the disaster would quantify what is needed to establish the value function. Further, interagency partners, such as FEMA, DHS, and the Red Cross, must be present to state their needs. These groups of experts capture the communication requirements pertaining to that scenario.

The second set of SMEs is known as system experts well versed in capabilities these systems deliver. Typically these are programmers, engineers, and acquisition specialists who intimately know the characteristics of NCE equipment. These SMEs can match the capability of these systems to the value function set by the operational SMEs. Though the capability-based model is to be system agnostic, eventually matching must occur as systems ultimately provide capability. However, this model limits the cart before the horse issue typically occurring in non-capability models, as the operator is present during the duration of the analysis, acting as an honest broker, constantly articulating operational need.

SME selection is often viewed as a lesser important duty of the process, but it requires meticulous record keeping to ensure SMEs are available and possess current and relevant knowledge. This requires recurring dialog between NORTHCOM, the SMEs, and their leadership to foster this network of personnel between planning cycles. This helps alleviate the cultural barriers in interagency forums, merely by conducting open and reoccurring chats to champion collective issues. This investment in social capital requires no formal design or procurement boards to establish. It is a simple exercise where leaders, SMEs, and planners pick up the phone or send an email to maintain contact and collectively work towards solving problems.

The Forum

An additional element of this process often overlooked is the type of forum used to capture prospective shortfalls. The JCIDS process is too formal and complex to facilitate a large interagency body. Often data calls are sent out beyond the confines of the headquarters without much facilitation, where SMEs and action officers remotely fill in spreadsheets within the walls of their cubicles. Hence a balance must occur where the forum is not too formal to stifle problem-solving, but not too relaxed an atmosphere as the *ad hoc* BOGSAT.

Initially, NORTHCOM should host the forum at its headquarters with a good facilitator to guide the process. Anything over a week in duration typically lacks productivity, as it will exceed human attention and interest span. The forum must be conducted in a true interagency fashion, with the right mixture of SMEs present from the respective agencies anticipated to participate in the given HLD/HLS scenario. The introductory session should include leadership from these agencies to champion the process and elicit support for it. After a few gatherings have been hosted at NORTHCOM, the forum could be rotated and hosted by one of the other interagency groups, further improving relationships and lowering cultural barriers.

The forum should be recorded to ensure the important sound bites have been captured and can be included in the findings of the planning session. Once the planning session is concluded by SMEs and planners, the packaged findings should be validated by the leadership of these various agencies. Again, this should be conducted in a collaborative setting, where collective buy-in and consensus is achieved.

This could serve as a seamless interagency planning process, where these senior leaders would present their findings to the house and senate in a true collaborative manner. Obviously it is absurd to assume 100 percent agreement amongst these diverse groups, but a mere 50 percent solution would be a far cry better than the current process.

Conclusion

The obvious solution to this problem is to consider the audience that will review the data. In this application, the audience will be at the flag officer and senior executive service rank. This implies that the time constraints of this group are precious and the process must be immediately understood to garner their buy-in. Analytical rigor is important, but not to the extent that a primer in network or engineering fundamentals is necessary to understand the results.

This is why a graduated scale of 1-5 is recommended to measure the performance of the attributes in the network-centric master capabilities list. Measuring availability in megabits per second versus available when needed has very little meaning to a career fighter pilot or infantryman. As operational experts will determine the value function, or the good enough value, of the model, it must be expressed in consumer terms. For example, when a consumer is purchasing a high-speed Internet connection for their home or office, few consumers know they need a connection speed of 1.5 megabits per second. However, they realize the need for a connection that is available when needed, reliable, and responsive.

Further, the overall CBP model must not contain too many moving parts. The current JCIDS model involves three distinct phases: the functional area analysis (FAA), the functional needs analysis (FNA), and the function solutions analysis (FSA). These are conducted in a stovepipe fashion; coupled with the ambiguity of the JFC and JIC, it makes for a far too complex model. Therefore, the design must be seamless and conducted in the same forum by the same SMEs to the greatest extent possible.

The ultimate advantage of capability-based planning is that it minimizes the BOGSAT phenomenon that resides in most military headquarters. CBP offers a model that has been vetted and scored by SMEs across many different disciplines from many different organizations. It

reduces making decisions in a vacuum and eliminates the emotional factor of funding pet rock programs. It is a process steeped in capabilities, not tasks or systems, which produce a quantifiable correlation to the shortfall, regardless if using a capability library or JIC for scoring.

The use of the scenario as the initial lens provides context, which is the most important phase of this planning process. It offers situational vignettes which provide flexibility when forecasting threat or adversary capability in current and out year planning cycles. It helps operators dial in their requirements and articulate specific capability needs.

The establishing of value functions set by the operator helps determine the good enough unit of measure in order to accomplish mission requirements. This helps eliminate gold plating that engineers tend to be fond of as they fall in love with their respective designs and systems. This should help restrain cost overruns and identify duplicate capabilities or areas that do not provide military value or utility.

What is useful regarding the proposed methodology, specifically addressing the master capability library, is in utilizing the four domains, i.e. air, land, sea, and space. This will call on experts from all branches of the service and interagency partners from the coast Guard, NRO, NSA, and NGA. This model will aid in the facilitating of joint and interagency collaboration and dialog.

CBP offers data that connects the dots between operator requirements, existing system capability, and what systems can bridge the shortfall gaps. It can aid in championing the utility of a system or it can provide quantifiable data that may justify program cancellation. For example, if a particular radio system is being developed and programmed, but it cannot be tied to an existing capability or future capability gap, decision-makers should question its utility and may desire to divert funds to programs that indeed can be traced to urgent capability needs.

In addition to making the model and process more intuitive across a wide body of operator and system SMEs, the measures of performance must be quantifiable and the justification of the score must be captured. Eliminating the complexity of the process, i.e. migrating to an MCL versus the JFC and JIC, would expedite the data collection processes considerable. It is well understood that planners desire a comprehensive model to ensure no stone is un-turned. However, the over engineering of the JCIDS process produces too much overhead and time spent to complete the planning process. In times of crisis, where SMEs are dragged out of their operational environment to participate in the CBP process, time and talent management is critical. Thus, a balance must be achieved to provide a reasonably feasible methodology that eliminates the ambiguity and time restraints associated with JCIDS.

This leads the discussion back to the overarching question of this article, which is: Does CBP possess the right methodology for defense planners and programmers in determining capability gaps/shortfalls? The emphatic answer is, if JCIDS is the approach used, no. JCIDS must be transformed to a simpler and more intuitive process. However, regardless of the methodology adopted, failure to conduct the planning session in an interagency environment will continue to provide myopic outcomes, with stovepipe solutions feebly provided to fill these gaps.

This research problem is inherently an interagency problem. Therefore, the problem-solving must occur in an interagency environment. Defense planning cannot continue to function in a vacuum. Cultural barriers must be leveled and this may be best motivated by controlling the purse strings. Interoperability standards should be designed into the planning, programming, and acquisition process. Interoperable engineering standards can then be validated before programs progress, ultimately being coordinated before an interagency working group.

This working group could participate in House and Senate appropriations committees to ensure the collective need is articulated and championed. Realistically then, for the culture to change via

the stick of controlling the purse strings, Congressional directives and oversight must occur to facilitate this change. Perhaps a derivative of the Nichols/Goldwater Act might be the instrument to force reform of the defense planning process. This initiative might eventually change the course of this bureaucratic and inefficient discipline.

In addition to legislative measures, a heightened awareness of the capability-based planning process must propagate within the DoD and its interagency partners. This may be facilitated by incorporating a training module in existing curriculums for action officers prior to starting their staff assignment. Further, recurring training could include a module of refresher training that could be implemented as an annual requirement. Familiarity training should also be made available to SMEs upon their selection to participate in a CBP forum. This could be a Web-based module completed prior to their participation in a CBP forum.

Perhaps more effective than familiarity training is a certification course, much like that which is encouraged for the acquisition community. This could act as an incentive for career planners and programmers to enhance their marketability and promotion opportunities. Further emphasis should be introduced into professional military education environments, such as: command staff and war colleges and civilian fellowship education programs.

One final recommendation of the overall CBP process would be to focus on non-material solutions to fill capability gaps. Though it is implied, too much emphasis is placed on matching systems to fill these gaps. Ample time must be spent on the entire DOTMLPF spectrum as a way to fill capability gaps. The obvious reason of why this fails to occur is that non-material solutions are less glamorous. Frankly, material solutions produce the most revenue and are more tangible to discuss and plan for. Optimizing business practices, which are normally tied to non-material solutions, should be the first area of house cleaning. However, in times of extraordinarily lucrative defense contracts, non-material solutions lose their luster.

Who Needs It?

Since capabilities are ultimately tied to programs and fiscal expenditures, CBP has its tentacles embedded into many organizations within the DoD. Currently the acquisition community, J5 and J8 embraces CBP, but other organizations have been slow to follow suit. Regarding communication and NCE gap analysis, J6 directorates across the DoD would benefit greatly if all were on the same sheet of music to adopt a standardized methodology. It is also imperative that these three directorates establish a more cohesive environment during the planning process. It is always disenchanting to discover that so few action officers have coordinated on NCE gap analysis across a headquarters organization. Every PowerPoint slide or talking paper must be reintroduced and explained *ad nauseum* for it to move up the bureaucratic ladder. Ironically, it is the financial management and comptroller community which understands CBP the least. While they are well versed at moving different pots of money around within the TOA, they seem less concerned about how the fiscal decision was reached to do so.

Ultimately, the entire J staff should be in lock step regarding CBP. Since NCE is such an enabling capability, every directorate is touched by its capability. Though the J5, J6, and J8 are the directorates responsible for conducting the process, the J1, J2, J3, and J4 are the primary stakeholders and ultimate recipients of NCE capabilities.

In addition to headquarter organizations, centers and agencies within the DoD could benefit greatly from the CBP model. First and foremost would be DISA. As DISA is DoD's executive agent for communications and NCE, DISA may provide SME support and senior leader oversight. The National Reconnaissance Office (NRO) is another obvious choice of an organization that could gain from the CBP experience. As dissemination of intelligence information obtained from the various space and sensor platforms, the NRO is critical to the defense of the nation and their

participation and advocacy in the CBP process is key. Ideally, NORTHCOM, DISA, the NRO, and DHS could form the nucleus to champion communication shortfall analysis for homeland defense. This collaborative model could be optimized over time, eliminating barriers and fostering effective relationships to solve this interagency problem.

About the Author

Kevin P. Wilson is a Major in the United States Air Force and a student in the National Security Affairs Department at the Naval Postgraduate School.

References

1. Ernest Forman and Mary Ann Selly, *Decision by Objectives: How to convince others that you are right*, 6.

2. Chairman of the Joint Chief of Staff Instruction 3170.01, *Joint Capabilities Integration and Development System* (2003), 1.

3. U.S. Air Force Instruction 10-604, *Capability Based Planning* (2006), 3.

4. U. S. Navy FORCEnet, *What is the Value-Added of FORCEnet*, 19 November 19, 2006, forcenet.navy.mil/fn-definition.htm.

5. Mike Connelly, Lieutenant Colonel, Deputy Director, Space and C4ISR Concept of Operations, AF/A5XC-SC, Pentagon, Washington, DC. Interview by Kevin Wilson. (2006). See also, Chairman of the Joint Chiefs of Staff Joint Functional Concept. Battle Space Awareness. Washington DC. 2003, Chairman of the Joint Chiefs of Staff Joint Functional Concept. Joint Command and Control. Washington DC. 2005, and Chairman of the Joint Chiefs of Staff Joint Functional Concept. Net-Centric Environment. Washington DC. 2005.

6. The Joint Chief of Staff, *The National Military Strategy of the United States of America, A Strategy for Today; A Vision for Tomorrow*, 2004, 19, 27.

7. Committee on Evolution of Untethered Communications, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications National Research Council, *The Evolution of Untethered Communications*, National Academy Press: Washington, DC, 1997, 1.2.5.

8. The JCS Glossary of Communications-Electronics Terms defines telephony/voice as: A form of telecommunication primarily intended for the exchange of information in the form of speech.

9. Ibid.: A point of interconnection to a network; One of the switches forming the network's backbone.

10. *The Evolution of Untethered Communications, Op. Cit.,* 1.2.7.

11. The Department of Defense, Joint Functional Concept, *Network-Centric Environment*, April 7, 2005, 1.

12. The Combined Communications-Electronics Board, Glossary of Communications-Electronics Terms, ACP 167(I), March 2005, 2-88

13. Joint Functional Concept, *Network-Centric Environment,* Op. Cit., B-2.

14. U.S. Air Force, *Master Capabilities Library, Net-Centricity*, Version 6.0, 2007.

15. Ibid.

16. ACP(I) 167, 2-171.

17. Ibid., 2-88.

18. *Master Capabilities Library, Net-Centricity*, Op. Cit.

19. Ibid.

20. Department of Defense, *Strategy for Homeland Defense and Civil Support*, June 2005, 3.

21. U.S. Air Force Fact Sheet, *Defense Satellite Communication System*. Accessed 5 April, 2007.

22. Ibid.

23. Joint Functional Concept, *Battle Space Awareness,* Op. Cit., 15, and *Net-Centric Environment*, Op. Cit., 6.

24. Chairman of the Joint Chiefs of Staff Joint Operating Concept, *Homeland Defense and Civil Support*, Washington DC, September 2006, 51.

25. Joint Functional Concept, *Net-Centric Environment,* 16.

26. Defense Information Systems Agency, *FY 2004/2005 Budget Estimate*, Research, Development, Test, and Engineering Budget Item Justifications, February 2003.

27. Chairman of the Joint Chief of Staff Instruction 3170.01, *Joint Capabilities Integration and Development System (2003)*, GL-4. DOTMLPF is defined as: doctrine, organization, training, materiel, leadership and education, personnel, and facilities; CDD is defined as: capability development document; and CPD is defined as: capability production document.

28. Chairman of the Joint Chief of Staff Manual 3170.01B, *Operation of the Joint Capabilities Integration and Development System* (May 11, 2005), GL-10.

29. Ibid., GL-9.

30. Ibid., GL-8.

31. The Joint Staff provides two definitions for Joint Capability Areas (JCAs): 1. An integral part of the evolving Capabilities-Based Planning process…the beginnings of a common language to discuss and describe capabilities across many related Department activities and processes, (SECDEF Memo, 6 May 2005). 2. JCAs are collections of capabilities grouped to support capability analysis, strategy development, investment decision-making, capability portfolio management, and capabilities-based force development and operational planning, (JCA Baseline Reassessment Terms of Reference).

32. The Department of Defense, *National Defense Strategy of the United States of America*, March 2005, iv.

33. Ibid., 11.

34. Ibid., 12-15

35. The Chairmen of the Joint Chiefs of Staff, *Joint Capability Areas 101*, J7/JETCD, April 2007.

36. The Joint Chiefs of Staff, *The National Military Strategy of the United Sates of America, A Strategy for Today; A Vision for Tomorrow*, 2004, 16-19.

37. Ibid., 16-19.

38. Ibid., 15.

39. NORAD/USNORTHCOM, *Strategic Guidance - Defending Our Homeland*, 1 December 2006, 1.

40. Ibid., 3

41. Ibid

42. Ibid., 5-6.

43. Ibid., 7-8

44. Ibid., 9.

45. CDRUSNORTHCOM*, USNORTHCOM CONPLAN 2501-05, Defense Support of Civil Authorities*, April 11, 2006, i.

46. Forman, Op. Cit., 5.

47. Ibid., 6.

48. Ibid

49. Malcolm Gladwell, *Blink: The Power of Thinking Without Thinking* (New York, NY: Time Warner Book Company, 2005.)

50. The Chairmen of the Joint Chiefs of Staff, *JOpsC Family of Joint Concepts - Executive Summaries,* August 23, 2005, 3.

51. Ibid., 5.

52. Ibid., 6.

53. Ibid., 11.

54. Ibid., 20.

55. Ibid., 4.

56. The Chairmen of the Joint Chiefs of Staff, *Capabilities-Based Assessment User's Guide*, December 2006, 4.

57. Ibid., 6.

58. NORAD/USNORTHCOM Instruction 90-144, *Capabilities Review and Resource Assessment*, November 1, 2006, 2-3.

59. Joint Functional Concept, *Net-Centric Environment*, Op. Cit., 4.

60. Brian Byrne, Program Analyst, Programs, Resources, and Analysis Directorate, NORAD/USNORTHCOM, N-NC/J81, Interview by Kevin Wilson, (2007).

61. Ibid.

62. Maria Grider, Branch Chief, Future Capabilities, Plans, and Policy Division, NORAD/USNORTHCOM, N-NC/J65, Interview by Kevin Wilson, (2007).

63. This methodology was my design while I was assigned to the Air Force Concept of Operations, AF/A5XC-SC, Pentagon, Washington, D.C. It was validated by the Air Force Communications Agency, Air Mobility Command, A3 & A6, Scott AFB, IL. The data derived from this methodology was published in the 2006 Air Force Capabilities Risk and Review Assessment and in Air Force Planning and Program Guidance. The NCE CBP methodology I propose is a tailored version of my original work to be used by USNORTHCOM to identify first-responder NCE shortfalls.

64. CBAM 101 Training, AF/A5XC-SC, Colonel David Johnson, USAF. (2006).

@inproceedings{Wilson2007DeterminingCS, title={Determining Communication Shortfalls for Homeland Defense; Strategic Insights, v. 6, issue 6 (December 2007)}, author={K. Wilson}, year={2007} }. K. Wilson. Published 2007. Engineering. Save to Library. The U.S. Department of Homeland Security will issue an advisory to American businesses, warning them of data security risks associated with using communications equipment and services from China-linked companies, Axios reported on Tuesday https://bit.ly/3mIiljp.Â FILE PHOTO: U.S. Department of Homeland Security emblem is pictured at the National Cybersecurity & Communications Integration Center in Arlington Virginia. (Reuters) - The U.S. Department of Homeland Security will issue an advisory to American businesses, warning them of data security risks associated with using communications equipment and services from China-linked companies, Axios reported on Tuesday https://bit.ly/3mIiljp. Its issue-area is traditionally narrowed down to military and defense affairs with nation-states as the sole actors. However, this customary trajectory of alliance politics is under change: Alliances of collective defense nature are increasingly giving way to security alliances that approximate collective security institutions.Â Recasting NATOâ€™s Strategic Concept Possible Directions for the United States Occasional Paper, RAND. 38.Â 2007. â€œThe Impact of Globalization on the Changing Nature of Warâ€, February 7, GCSP Policy Brief No 24, Geneva Centre for Security Policy, Geneva. 29The point also explains the logic of â€˜the mission determines the coalitionâ€™ statement, which is much discussed in the run-up to the wars in Afghanistan and Iraq, in 2001 and 2003 respectively.