12TH ICCRTS
"Adapting C2 to the 21st Century"

Beyond PowerPoint Deep: a Concept of Operations for Implementing Net-Centric Warfare

Topics:
Track 1: C2 Concepts, Theory, and Policy
Track 2: Networks and Networking
Track 7: Network-Centric Experimentation and Applications

Lawrence P. McCaskill

POC: Lawrence P. McCaskill
Chief DoDAF Architect
Whitney, Bradley, & Brown, Inc.
1604 Spring Hill Rd, Suite 200
Vienna, VA 22182
703-448-6081 x127 (Larry McCaskill)
lmccaskill@wbbinc.com

In working on various Net-Centric Warfare (NCW)-related projects, I've encountered varying interpretations of what it means to be "net centric." OASD/NII and DISA are developing the primitives that programs are supposed to leverage during their transformation from "platform-centric" to "net centric" through their ongoing developing the Global Information Grid (GIG), the Net Centric Operations and Warfare Reference Model, and Net-Centric Enterprise Services (NCES), respectively. In helping to make this transformation, they are "doing yeoman work," but as yet, haven't developed a document that explains their vision of NCW "to the rest of us." What's needed is something that ties all the hyperbole about NCW together into a coherent description of "how NCW is supposed to work" that goes beyond "buzzwords and bumper-stickers" (horizontal fusion… machine-to-machine interfaces… smart pull… etc.). Therefore, what I will attempt to do in the following pages is provide a lucid concept of operations of how NCW *could* work, leveraging the current efforts and paradigms being used by DISA and OASD/NII, and go a layer below the "lightning bolts" contained in most of the NCW-related "propaganda" on the streets. It will not necessarily be *"THE"* method the DoD uses to implement NCW, but will provide the reader a point of departure for understanding and discussing NCW-related issues.

WHAT IS NCW?

In their book ***Network Centric Warfare***, Alberts, Garstka, and Stein defined NCW as:

> …an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. In essence, NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace…
>
> (Source: **Network Centric Warfare,** Alberts, Garstka, and Stein, CCRP)

Since this book was published, the policymakers at OASD/C3I (since renamed to OASD/NII) have shortened the term to "Net-Centric Warfare," in order to de-emphasize the "network" in it, as people were confusing "network enabled" with "network centric" (the key distinction there is just because you're "robustly networked" does not mean you're "net centric" – one enables the other, but just because you have the former, doesn't mean you have the latter).

OK… you've started out by telling me just because I have a robust network, that I'm not net-centric… how do we achieve the "net-centric" in NCW?

NCW, in large part, is using ubiquitous, robustly networked sensors tied together in a publish-subscribe environment to enable increased situational awareness via increased speed of command brought about by automated processing of the information provided by the ubiquitous sensors into "actionable" information (yes… that's a mouth-full). This will be accomplished by using rules-based systems, enabling predetermined actions to take place via the matching of patterns (this, in NCW parlance, is called either "swarming" or "self-synchronization"). This will enable several decision support systems, built on the "command by negation" construct, to automatically take action without operator intervention for many of tasks where operator intervention isn't required (resupply, non-lethal self-protection, etc.). However, especially in the

case where lethal means are being used, I envision explicit operator approval will be required to initiate "bombs on target;" however, the decision support system will enable faster course of action determination via recommendation of viable courses of action using rules-based automated means.

NCW, as the DoD envisions it working, is based on the leveraging of technologies in wide use in web-enabled business-to-business (B2B) transactions. The technical term behind the technologies associated with B2B transactions is called either "Service-Based Architectures" or "Service-Oriented Architectures (SOAs)," with the latter being more popular. Businesses use this technology to facilitate "just in time" delivery of products, thereby eliminating the need for large warehouses. An example of this is how Wal-Mart operates business: each Wal-Mart store is networked together, and each night, the sales figures from all stores are sent to headquarters. Wal-Mart has prearranged contracts with the vendors of the items they sell that allow them visibility into this data, as well as an arrangement to automatically initiate shipment of items directly to stores when a particular item's stock (that the vendor produces) has become depleted. A concrete "for instance:" if a Wal-Mart in Anytown, USA is about to sell out of paper towels, the paper towel manufacturer, via visibility into Wal-Mart's databases, determines that the stock of their product is below the agreed threshold level at the Anytown, USA store, and automatically initiates shipment of more paper towels to the Anytown, USA store. This happens automatically, without the Anytown, USA Wal-Mart having to manually place an order for more. Manufacturers of products, to include Caterpillar and Toyota, among others, have similar agreements with their parts suppliers, enabling them to predict when parts will be needed from historical data, as well as to have the correct inventory available for delivery to the manufacturer.

These B2B transactions are enabled by web-based portal technology. *What's a portal?* Web portals are essentially agreed-upon entry points into internets/intranets (i.e., a website, defined by a Uniform Resource Locator or URL – the website address). Commercial examples include Yahoo, MSN, and AOL. These portals include commonly used services and applications including search engines, directory services (white and yellow pages), news, email, stock quotes, maps, forums, chat, shopping, and options for profile-based customization to let the user pick how they want their user interface to look. Applying this to the NCW, think about a corporate intranet; it has the same type of services, but these are only available to specific people who have been granted access to the site (usually via username/password/profile security mechanism). Additionally, portals for NCW are generally a specialized type of portal called an **Enterprise Knowledge Portal**, which is an enhanced Portal that:

- Is focused on knowledge production, knowledge integration, and knowledge management
- Focuses upon, provides, produces and manages information about the validity of the information it supplies
- Provides information about your business/warfighting area and information about the degree to which you can rely on that information
- Distinguishes knowledge from mere information
- Provides a facility for producing knowledge from information (services)
- Orients one toward producing and integrating knowledge rather than information

Recognizing that enabling Net-Centric Operations requires one to have compatible and/or common web-based services, the Defense Information Systems Agency (DISA) has been

directed to develop a core set of web-based services for the DoD Enterprise (additionally, DISA's commander has now been tasked with the following responsibilities: Commander, JTF-Global Network Operations and Deputy Commander, Joint Force Headquarters-Information Operations for NETOPS and Defense or US STRATCOM, and is responsible for providing operational support of and security for the GIG). The program under which these are being developed is called "Net Centric Enterprise Services" (NCES), and was started in FY04. An initial set of core services have been identified, and are being developed by inter-service, inter-agency teams. These are being called NCES Core Enterprise Services (NCES CES); these include (9):

- Messaging Services: Ability to exchange information among users or applications on the network (e.g., Email, DMS VMF, USMTF, TADIL, OTH, Message Oriented Middleware, AOL instant messenger, Wireless Services, Alert Services)
- Discovery Services: Processes for discovery of information content, people, or services that exploit metadata descriptions of network resources stored in Directories, Registries, and Catalogs
- Mediation Services: Federation of services that helps users mediate, fuse and integrate data. Types of Mediation:
    - Adaptation: Used when an invoking application cannot communicate directly with an outside service. Adaptors provide service mediation when systems need to communicate point to point.
    - Orchestration: When a service request triggers a whole chain of events, orchestration services assemble and manage the integrated services (workflow).
    - Transformation: When an application requests information that is not available in the fashion that the requestor desires, transformation services convert the information into the desired format. This will probably be the most prevalent form of mediation.
    - Aggregation: Provides a central point of interaction when requesting information. There are usually multiple information sources points being integrated into the single point of interaction.
- Collaboration Services: Allows users to work together and jointly use selected capabilities on the network (i.e., chat, online meetings, work group software etc.).
- Application System Management (ASM) Services: Provides for monitoring and repair of network resources
- IA/Security Services: Federation of information assurance and security capabilities that addresses vulnerabilities in networks, services, capabilities or systems.
- Storage Services: Physical and virtual places to host data on the network with varying degrees of persistence (e.g., archiving, continuity of operations [COOP], content staging)
- Enterprise Service Management: enables life cycle management (planning, design, developing, organizing, coordinating, staging, implementing, monitoring, maintenance and disposition) of all the capabilities of, and services provided by, GIG Enterprise Services (GES), thereby enabling NETOPS of GIG systems, networks, and their defense, through standard technological solutions (people, tools and integration).

Why would we want to leverage portal technology? Historically, information in the military has been "stovepiped." To gain access to information, one had to go through the "chain of command" in order to gain access to information, or to specific organizations that "owned" the information (e.g., the intelligence community). Historically, intelligence information has been

produced using a paradigm called the "TPED" process, and involved **T**asking an intelligence asset to gather data, **P**rocessing the data into useable format, **E**xploiting the data to provide "actionable" information to the warfighter, and **D**isseminating the information to the warfighter. While the model seems logically viable, in practice, due to the sheer amount of information collected, there were bottlenecks created between information collected via taskings, vs. available analysts to process and exploit the information. Thus, much of the collected information "stayed behind the green door" until it was processed and exploited by intelligence personnel, creating situations where by the time the information was disseminated to the warfighter, it was "technically correct, but three days too late to do us any good…" Additionally, although the intelligence information was collected with a specific intelligence purpose in mind, it could have been used by other organizations prior to processing and exploitation. This created islands of information that, in the endgame, were inefficient – the warfighter wasn't getting the information he required, even though it was already "out there somewhere" and had to either "make do with the awareness level he had," or task his own assets to gather further information.

In order to "fix" the problem of "islands of information," a "new way of doing business" will have to be adopted. This was the subject of the Deputy Secretary of Defense Management Initiative Decision 905, and the concept is being called "TPPU" (pronounced "tee-poo") and involves **T**asking of the intelligence gathering assets, **P**osting the results of that information gathering, **P**rocessing the information for the purpose which is was gathered, and **U**sing the information.

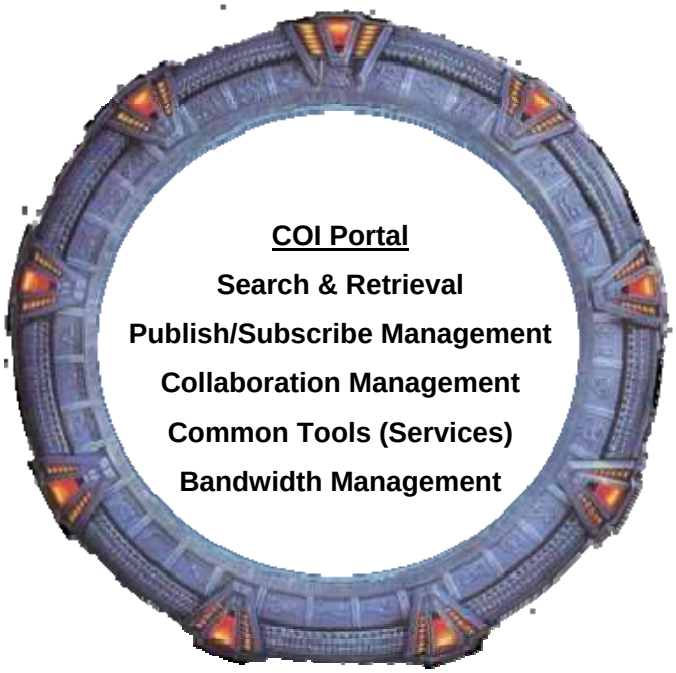
OK…great… post it where? How are we going to find this stuff? To get to the point where this can be completely answered, we need to first talk about some more NCW buzzwords.

The first concept to introduce is that of the community of interest (COI). A COI is the collection of people, assets, and organizations that are concerned with the exchange of information in some subject area. Examples of possible COIs are:

1) A Joint Functional Capability (or specific missions providing the capability)
2) Multiple missions with a common goal (example: a strike package)
3) A specialized mission area (example: time critical targeting)

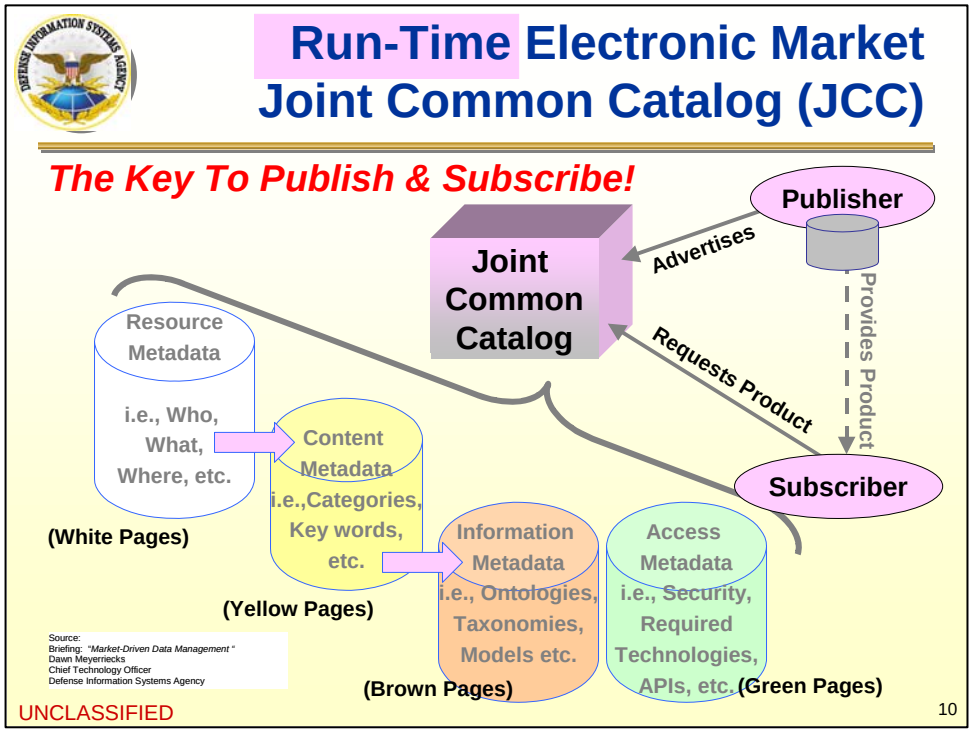
DISA envisions three types of COIs:

1) Expedient (ad-hoc) COIs
2) Institutional (predefined) COIs, usually mission-based
3) Cross-functional COIs



One gains access to a COI through the COI-based portals. As discussed earlier, the portal is an agreed-upon address through which one gains access to COI information and services, and can be thought of as being similar to a company-based intranet in that they provide a window into corporate information, have web-based tools (services) available for use, and can have the ability to tailor the "look and feel" of the interface based on user profiles.

The end-user gains access to COI information via interfaces to specific COI services; some example services that will eventually be "universal" are as follows:



1) COI Search: searches the catalogs of the COI, and provides information to the requesting entity based on the following metadata (data about data) within the COI catalogs:

   a) Resource Metadata (White Pages): Who produced the information; this is required to maintain information "pedigree."
   b) Content Metadata (Yellow Pages) Categories, Key Words, describing the content of the information.
   c) Information Metadata (Brown Pages) Ontologies, Taxonomies, Models that describe the formatting of the information. These will enable Mediation Services to translate information for different end-user devices and applications.
   d) Access Metadata (Green Pages) Security, Required Technologies, APIs, etc.

When your favorite "computer geek" talks about "tagging" the data, this is what they mean. Tagging the information provides the contextual information related to the environment within which the data is created. An often-used example of this is a tank; in Army parlance, a "tank" is a tracked vehicle, while in the Air Force communities - the ones that don't define a "tank" as a "target" - a "tank" is something that holds fuel. The context in which the "tank" is being used provides its true meaning. The communications community (in particular, DISA) has been trying to "fix" this problem for years via attempts at data standardization, and via attempts at providing a centralized "translator" (called the "SHAred Data Environment" - SHADE - CORBA [Common Object Request Broker Architecture] and COM [Common Object Model - Microsoft] were proprietary implementations of SHADE). These technologies were only sparingly used due to high

cost of entry, and due to each of them being proprietary. The latest technology that obviates the need for these proprietary tagging technologies is XML (eXtensible Markup Language). XML is a tag-based, hierarchical markup language for description of data and its relationships. Contrasted with HTML (HyperText Markup Language – the language specified by typing "http" at the beginning of an address in your web browser), which has fixed-meaning tags (usually format-related) embedded in document (in your web browser, hit View => Source to see the tags in the document), XML allows the user can define the tags which are used to describe data in a page. XML tags are "standardized" in communities by definition of Namespaces. Within the DoD, namespaces being managed by DISA on the DoD Metadata Registry and Clearinghouse website (note: for non-DoD users, a PKI certificate is required to view this site):

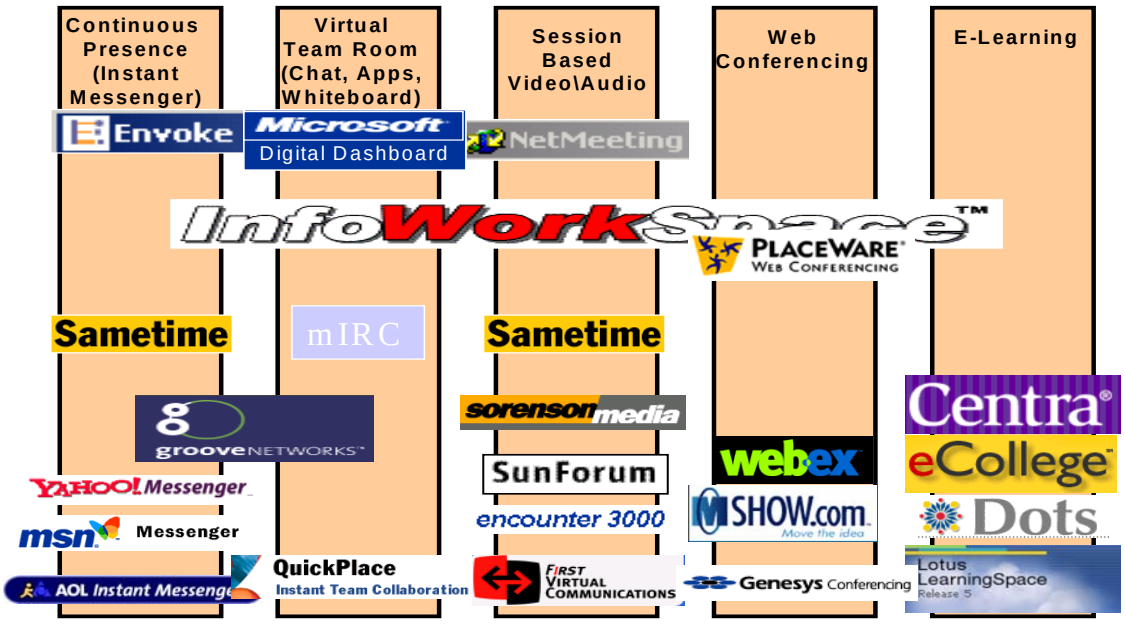
https://metadata.dod.mil/mdrPortal/appmanager/mdr/mdr

Namespaces have been "binned" by predefined "communities of interest" (COIs -- Command and Control, Intelligence, etc.). Therefore, each COI must have a steward that is responsible for maintaining the definitions of the namespaces within the COI. The standard format for XML is unicode, which in most implementations takes 16 bits per character (ASCII takes 7 or 8, depending upon implementation), which may have implications on the size of information being transferred, but several data compression techniques have been used to mitigate this effect. Several XML-based technologies for defining available services and protocols for communication are in development (WSDL, SOAP, DAML, ebXML, SAML, UDDI); see http://www.oasis-open.org/home/index.php and http://www.w3.org/XML/ for more information.

2) Retrieval: gets data either from the COI "enterprise-level" datamart, or from Sub-COI Datamarts and Datastores. This implies that COIs (at least from a cataloging perspective) are hierarchical. This is described in more detail later in this document.

3) Publish and Subscribe Management: publish and subscribe management can be thought of as being much like what is provided commercially today by such services as automated stock tickers, weather reporting, and "show me what is going on at a camera station" programs (Pointcast, Infogate, Trafficland, and WeatherBug) – they provide a smart, filtered push of information as it changes within the COI, based on filters and attributes selected by the user on either an ad-hoc basis, or via a user profiles (discussed in more detail later). This is the basis of the "next generation" of the "Common Operating Picture" (COP) called the UDOP (User-Defined Operating Picture).

4) Collaboration Management: collaboration management between entities both inter- and intra-COI. Chat rooms are with whiteboards and shared applications are examples of this capability. Within the DoD, the DCTS (Defense Collaborative Tool Suite) is "bridging the gap" between vendor tools via provision of standard collaboration interfaces and formal acceptance testing. Examples of vendors providing applications in this tool space:



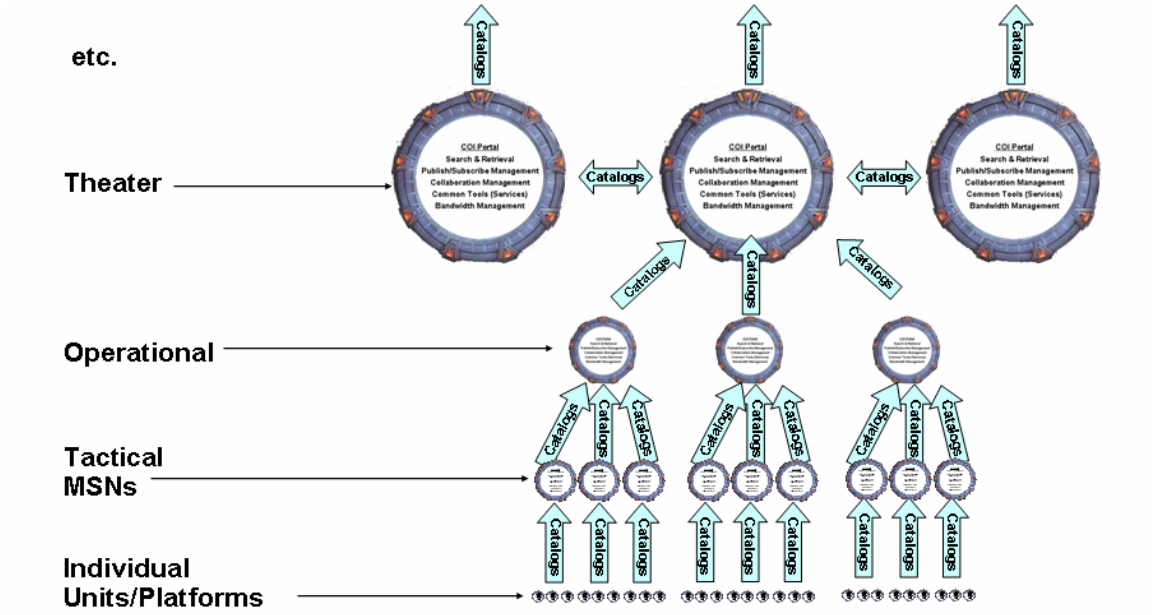
Collaboration Tools

5) Common Tools (Services): each COI will have tools that are common to it, but not necessarily other COIs. These will be accessible here. These common tools are referred to as "Services" within the construct of Service Oriented Architectures.

6) Bandwidth Management: while it is possible that this will be implemented in one or more of several different places (i.e., it may not necessarily be implemented by the portal), bandwidth will need to be managed in order to provide the equivalent of the priority system on Autodin/Defense Switching Network (DSN). An emerging technology that will enable this to happen will be IPv6 (Internet Protocol, version 6), which will make allowances for priority-based schema for message delivery.

Regarding COI catalogs, let's defray a common misinterpretation regarding NCW and the GIG: the GIG (and by extension, NCW) ***is <u>not</u>*** built on the assumption that "due to infinite bandwidth, we'll be able to have all the information everywhere all the time." What it is about: is gaining tailored, filtered access to information as it's created, using publish-subscribe technologies, which are able to find the information needed via catalogs. In order for the publish/subscribe mechanism to work efficiently, it needs to make use of data and service catalogs. The two major schema regarding cataloging in the internet environment are peer-to-peer and hierarchical. Peer-to-peer cataloging technology requires some degree of anonymous catalog information gathering

by “web crawling” engines; due to the high security environments in which the NCW environment will exist, as well as the limited bandwidth environment, I don’t think this technology is viable for NCW. That leaves hierarchical catalogs; within hierarchical cataloging constructs, each COI maintains information for its COI. COIs will propagate their catalog information to higher echelon COIs until the highest COI within the business or warfighter domain is reached. This allows for well-known entry points to be created for specific types of information and services. At higher level echelons, the potential exists for catalogs to be propagated across “same level” echelon COIs, but I believe the implementation for most catalogs will be hierarchical.



COI Catalogs Propagate Hierarchically:

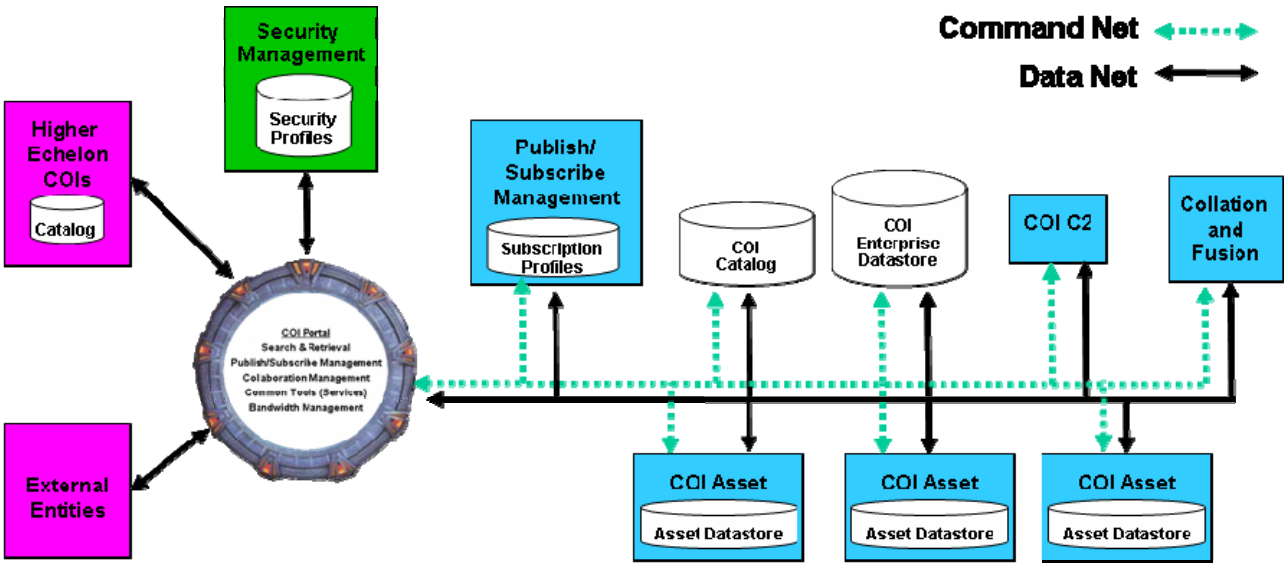
– Catalog data is propagated up the chain

– Only catalog info propagated rather than “all information everywhere” all the time

– High-echelon catalogs *may* propagate horizontally

Key point: there are other schemes for catalog management, but this allows for manageable “catalog by hierarchy,” and horizontal fusion via publish-subscribe mechanism

PRACTICAL APPLICATION



Now, let's get started on the meat of "how this works." Each COI contains the following datastores:

1) COI Enterprise Datastore: contains "cooked" or processed data that has either been produced as part of the normal COI functioning process, or Collated and Fused via the COI-specific Collation and Fusion functionality
2) COI Common Catalog: contains lookup lists of all information in the COI, to include subordinate COIs.
3) Asset Datastores: as previously alluded to in the discussion of how catalogs propagate, COIs can be nested. A key point is that an entity can subscribe to both "cooked" information from the Datamart, or "raw" data from one of the sub-COI Datastores (which can be Datamarts for the sub-COI, or individual asset data storage). This "raw" data subscription is how TPPU will be implemented.

COIs, as stated before, are maintained based on shared interest in information associated with a subject or mission area, with the primary goal of being tailored, filtered information to the end user via shared services such as publish and subscribe. The COIs can have default membership, or one can request membership. However, this implies two interrelated services: profile management and security management.

1) Profile Management: the primary mechanism via which the portal mechanizes the publish/subscribe function for the user is via the user profile. The profile contains such information as security clearances, information subscribed to, COI membership, etc.

2) Security Management: when an entity wishes to gain access to the COI, it first must go through the COI Security Management service. If access bona fides are not met (using the Profile Management service), access is denied. If access to the portal is granted, the entity may engage in any of the services available via the COI portal based on the match between the clearance and the services available to that clearance.

Referring back to the diagram, 2 buses are depicted:

1) COI Command Net: a data bus for inter-COI information exchange. All services within the COI monitor this data bus for commands addressed to it

2) COI Data Net: data is put on the COI data bus in response to a retrieve request. For data exiting the COI, this allows the Retrieval function the ability to "manage the pipe" exiting the Information Manager, ensuring highest priority data moves most quickly.

These two networks provide the backbone on which the other services related to the COI send information to one another. Now… let's describe the services:

1) Subscription Service: the subscription service is handled by "Publish/Subscribe Management" within the diagram. The goal of this service is to provide tailored information to the subscriber. Webster's defines subscription in two ways:

    a. To enter one's name for a publication or service
    b. To receive a periodical or service regularly on order

    Within the context of this discussion, we mean "both," but primarily the former – by subscription, we mean: to register to be the recipient of a distribution of information upon its creation and subsequent updates; the subscription can be to either processed (or "cooked") information (e.g., imagery with notations and analysis applied to it), or "raw" data (e.g., non-annotated imagery directly from the source).

    Based on the profile assigned to the user, there are de facto subscriptions to information as well as the potential for ad hoc subscriptions to take place and be serviced based on the access rights available to the profile. Regarding the de facto subscriptions, when an entity has gained access to the COI (via interface with Security Management), the Subscription service knows the entity is available to receive information. Additionally, the subscription manager needs to be able to track "as of" times in the case of entities that connect and disconnect regularly from the community (tactical platforms, ships, etc.).

    What's contained in a subscription? Subscriptions include the type of data, information related to the pedigree of the information, and means by which the information is made available to the user (for instance, the entity may want the data produced, or it may only want notification that the data is ready for consumption). The subscription can also include information relating to the acceptable formats receivable for a user (the paradigm to think of here is the "disadvantaged user" with limited bandwidth; his subscription includes the identification of formatting/tailoring of information for him to receive it using his end-user

device).

The Subscription service monitors the COI Control Net for Asset Status messages/updates, which contain the cataloging data associated with the updates. With this information, the Publish and Subscribe Management function takes each status update and compares it to the Subscription List. If the Publish and Subscribe Management Function determines that this new information has been subscribed to (without having to retrieve it), it sends this information (i.e., a notification that new information is available) directly to the subscriber. If the subscriber has automatically subscribed to the actual data (vs. merely a notification that new information is available) associated with the update, the Publish and Subscribe function sends a Retrieval Request to the Retrieval function, which retrieves the data, and passes the data on to the subscriber, tailored based on the filters set during the subscription process.

The Subscription Service also uses Asset Status messages/updates to update the COI Common Catalog. Upon COI Common Catalog Update service, it submits these updates to Higher Echelon COIs. This is depicted in "COI Catalogs Propagate Hierarchically figure.

We've talked a lot about subscription services; now let's talked about Publishing; within the construct we're developing here, the following definitions of "Publish" apply:

- Advertise: make information available for consumption. Includes development of all catalog information (White, Yellow, Green, and Brown Pages metadata)
- Distribute: to service the subscription list
- Post (Asset Status): to make available information on the status of an asset (location, system/subsystems status, fuel status, etc.), to include indications that new information is available (imagery, etc.) for:
  - Advertisement
  - Distribution
  - Aggregation/Analysis

In the endgame, the Publish/Subscribe function provides for the functionalities described above.

2) Data Collation and Fusion Service: if the trigger to collate and fuse the information is to be automated (which is desirable; otherwise, this will have to be accomplished on a situation-by-situation basis via human intervention), the decision of which information is to be queued for collation and fusion at the portal level is determined in the rules regarding COI formation. Assuming this has been automated to some degree, upon examining the Asset Status messages/updates, if the rules regarding the Asset Status messages/updates dictate retrieval of the information for use in collation and fusion, the Collation and Fusion service requests data from the Asset owning the information, as well as current data from the COI DataMart, in order to collate and fuse the data (this assumes a "notify, but don't send" subscription to the data, rather than "send it directly" subscription). Upon finishing the collation and fusion of data, it passes the data to the COI DataMart for storage. The COI DataMart then publishes an Asset Status update message, which passes information to

Publish and Subscribe Management that gives it the requisite cataloging information to update the COI Common Catalog.

3) Search: an entity, after gaining access to the COI via interface with Security Management, may perform ad-hoc searches of the COI Common Catalog. The information that gets passed on "hits" are views tailored to the entity's function as well as clearances. Information associated with the "hits" white, yellow, green, and brown pages' information are tailored and presented to the entity, such that it is possible to select one or more of the information sources for Retrieval.

4) Retrieval: the Retrieval function can take as input addresses provided by either the Search function, or via information provided by the Publish and Subscribe function (during the "Tailored Data to the Subscriber" process). The function then puts out a Data Request on the COI Control Bus, which is picked up by the addressed Asset and processed. Upon processing, the data is placed on the COI Data Bus, which goes back to the Retrieval function for tailoring based on entity attributes, and then gets sent to the Entity in the form of Ad-Hoc Request Data. Once again, none of this can happen unless the Entity has gone through the gaining access to the COI via interface with Security Management process.

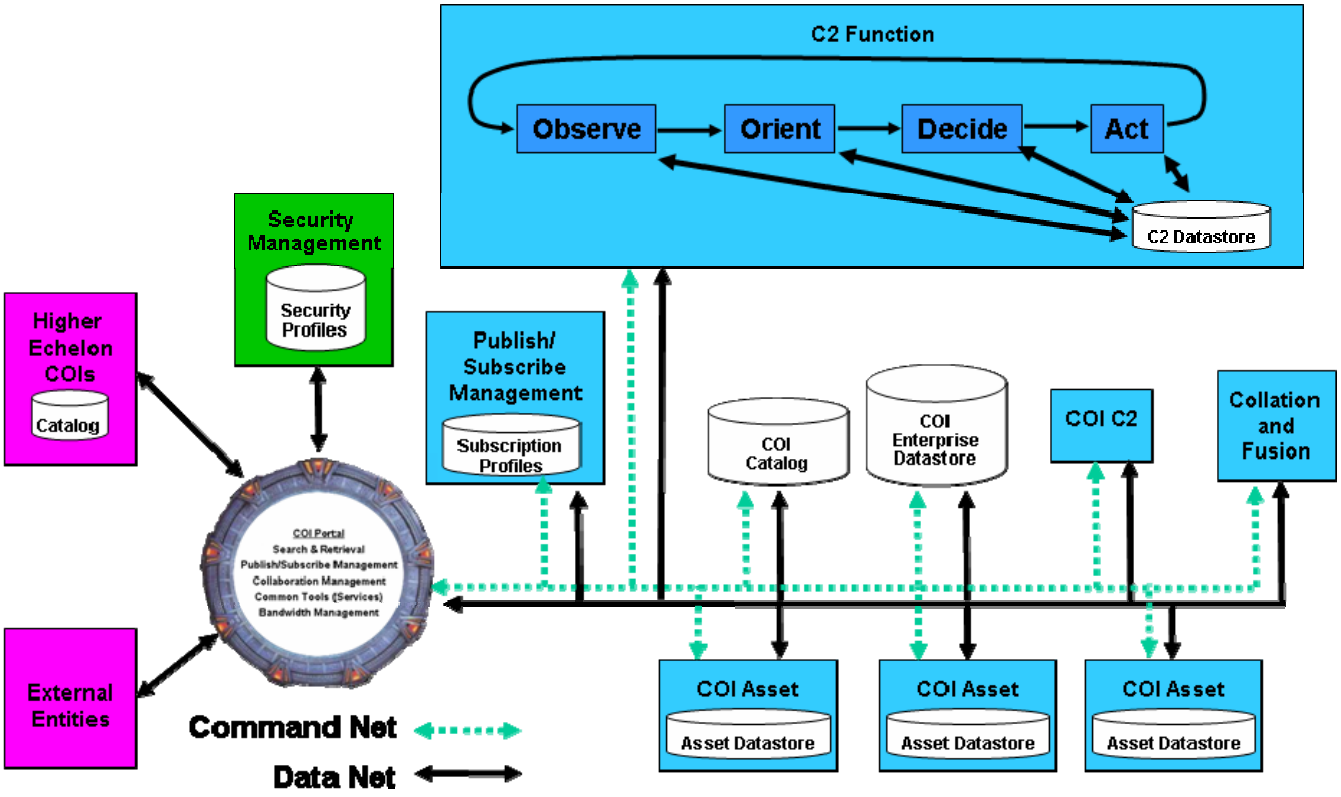
5) Collaboration: An entity, after gaining access to the COI via interface with Security Management, may register/request for collaboration with COI assets via Collaboration Management. If the request is granted, the entity is sent a request for collaboration, which includes mechanism to connect to (via Collaboration Management function), available applications, protocols, membership, etc. Via this "signup" process, the connections are formed such that collaboration can happen; the Collaboration Management function processes the transmissions from each of the collaborating members, and translates the messages based on the tools being used to collaborate, and then forwards these messages on to the entities' and assets' end-user devices for processing.

THE MONITORING LOOP

We've described the constituent parts of a COI, and how they operate individually, but what does this COI construct allow us to do as a model of an overarching system?

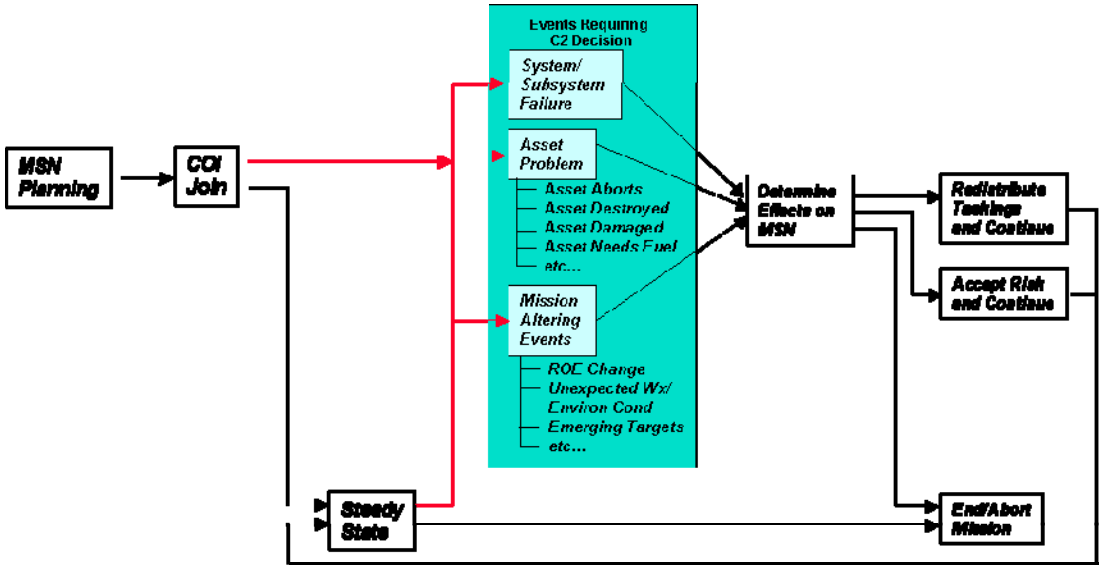
A COI can exist anywhere from the individual user/platform all the way up to a nation; the key point is COIs are composeable, and that each COI has some degree of "normative behavior." Using the COIs as the main organizational construct around which these "normative behaviors" are organized performs the following functions:

- Allows one to identify candidate roles around which to build constructs to facilitate collaboration. This allows the collaboration tool/service vendors to configure their respective products correctly in order to organize their products most appropriately for COI use.
- Allows one to create automated engines to facilitate decision loops within each COI. These types of constructs and/or processes are critical to performing operations utilizing "centralized control, decentralized execution" via allowing each COI to self-synchronize and perform what in military parlance is called "type orders." In accomplishing these "type orders" (e.g., reconnoiter an area looking for SCUD missile launchers) allowing for emergent behavior that accomplishes the task at hand more quickly and efficiently than traditional command-and-control based structures.



C2 Function as a COI Service

Expanding on the 2nd idea above, each COI has a command and control service, which executes a decision cycle. The decision cycle modeled (OODA, MAPE, See/Decide/Act/Finish Decisively, Alberts/Garstka's net-centric decision model, etc.), really doesn't matter. Via use of the decision cycle, COI C2 can react to changes within the COI. This presupposes that one is using an event-driven paradigm, an example of which is included below:



Event Driven System Example

During mission planning, one determines the parameters associated with the mission, including the conditions to watch for that would take one out of the "Steady State" above. After joining the COI (effectively a communications handshaking process, which identifies your assets to the COI and provides one with current situational awareness of other COI members and information related to the mission, etc.), so long as mission execution is going according to the plan, one remains in Steady State. However, when conditions occur that could potentially cause one to alter the course of the mission via reapportioning assets, aborting the mission, or accepting risk to continue the mission, a decision must be made. Upon making the decision, the execution of the resultant plan becomes the Steady State.

In mechanizing this decision loop process, one would create what amounts to a "polling loop" whereby the COI assets are polled for changes to its asset since the last report. The reports of these changing conditions are collated, fused, and decided upon as follows:

Observe:

> The Observe function operates on watch indicators decided upon during Mission Planning or subsequent mission updates. As part of its functioning, it tracks the status of entities of interest to the COI (friend, foe, other), and monitors for occurrence of specified events (both inter- and intra-COI). If events it is monitoring for could happen outside the COI, it subscribes to notification of these via the Publish and Subscribe service. Upon detection of an event of interest, the appropriate information is collected (based on the type of event detected), and passed to the Orient function.

Orient

The Orient function determines how the events shaping the current status happened, and what effects (primary, secondary, and tertiary) the events will have on the current status. Stated another way, the Orient function puts the changes occurring in the COI into context for the decisionmaker, and publishes this analysis for consumption both inter- and intra-COI. This starts the Decide phase.

Decide

The Decide function takes the information in derived in the Orient function, and decides the appropriate course of action. As previously stated, these courses of action can range from accepting risk and continuing the mission, reapportionment of assets to address the occurrence of new information, and possibly even aborting the mission in its entirety. Assuming the mission is not aborted, the output of this step is the new mission parameters, including orders and watch conditions that the Observe function will monitor. This puts one into a concurrent state of "Act" as well as Observe.

Act

Within this construct, Act and Observe occur concurrently. One remains in Steady State so long as the actions being taken fall within the parameters set out in the mission plan. Any results of action are passed on to the Observe function, which performs the pattern matching via monitoring of Watch Indicators to begin the decision cycle over as required by changing events.

The C2 Datastore:

As is true with the other COI assets, the COI C2 has a datastore. Upon update of any C2 COI/mission area information, the COI Publish/Subscribe is notified that information has changed, and the information is processed using the rules established for the COI.

SERVICES

Up to now, we've been addressing an information-based, publish/subscribe services environment; as was covered earlier, DISA has a set of services that they are developing, and it is envisioned that each COI will offer services unique to the COI. Each service can be described using an extension of XML called WSDL (Web Services Definition Language), and thus cataloged, much as information catalogs have been discussed previously. Most simply put, it's a description of what the service is, what inputs (and in what formats) it expects to see, and what formats it outputs data.

Thus, subscribing to services follows the same paradigm as subscribing to information, as discussed above. Additionally, the services are being designed such that they are "composeable" – i.e., one can combine several services together and offer them as a "super service." However, that is beyond the scope of this paper.

A CONCRETE EXAMPLE/SAMPLE VIGNETTE

This vignette will show how these concepts can be leveraged to provide will be a "non-traditional intelligence, surveillance, and reconnaissance" (NTISR).

A fighter aircraft scheduled for an aerial combat patrol mission has a sensor with which it can provide imagery (synthetic aperture radar, electro-optical, or otherwise); the pilot wishes to make this asset available to the "greater community," as he only uses it during strike engagements, none of which currently scheduled for his current mission. As it leaves the airfield and flies enroute to the patrol area, the aircraft "reports in" to the airborne network, giving the status of its on-board equipment (i.e., sensors, etc., and the potential services these systems can provide). During this reporting in phase, via a pre-determined profile, the pilot and/or aircraft has subscribed to such things as: new threats discovered, new targets available to be serviced, location/status of friendly aircraft, etc.

A commander of a ground unit requires current imagery of an area that he will be responsible for occupying and patrolling. He goes to his current imagery resources, and determines these are dated, due new construction, buildings being destroyed, obstacles being placed during conflict, etc. Via connection to an imagery service, he submits a request for current imagery within his patrol area.

An ISR collection manager receives the request for current imagery in an area under the purview of his control. The ISR manager looks to see what assets are available to service this request, and selects the fighter aircraft on patrol. This selection generates a request to the fighter aircraft to take a picture of the area, and send the image to the ground unit commander as well as the ISR manager (who will ensure the image is loaded into the imagery server, enabling its use by others in the future).

The fighter aircraft acknowledges receipt of the tasking, and WILCO's (since NTISR is a secondary mission for the patrol aircraft, the pilot has the ability to nonconcur with the request, which might happen in the case where the pilot has been tasked to accomplish a higher priority mission). The ground commander and the ISR manager are made aware that the request is being serviced, and an expected time that the image will be available. Upon imaging the target area, fighter aircraft posts the image, making it available to the network. Both the ISR manager's system and the ground commander's intelligence system are subscribed to this information, and automatically submit requests to the aircraft to send this information. Within the COI portal, this is where a priority schema will have to be invoked – in this case, it's probably more important to the ground commander requesting the image than the ISR manager to have the image "in his hands – *NOW*." Thus, the aircraft sends the information to both users, with more priority being given to the ground commander, and presented in a format the ground commander can use (a potential segue: if the aircraft collect an image that isn't in a format the ground commander can use, but that the ISR manager can convert using some sort of mediation service, it may be sent to the ISR manager for conversion, prior to being sent to the ground commander). Upon being transferred to the ground commander's system, he is alerted via any of a number of means (instant message, e-mail, etc.). Upon being distributed to the ISR Manager's system, it is fused with current information, and made available to other users; this would enable the information to be saved and available to the network when the fighter aircraft leaves the area and returns to base (thereby removing its "datastore" from the available cataloged assets within the COI).

Some salient points:

- This vignette implies that, prior to accomplishment of any such mission, constructs are in place for security services, profile management, catalog management, etc. The implication here is this stuff doesn't "just happen" – it requires funding, manning, etc.
- Prior to submitting the "want ad" for new imagery, the end user will have checked existing resources to ensure there isn't imagery available that meets his needs. Services such as Image Product Library already provide a similar capability. The "want ad" service could be an extension of such a capability.
- The end user will have had to log onto the network, providing bone fides, which will be used by the ISR manager to pair his needs with assets available.
- In submitting the "want ad" for new imagery, prior to servicing the request, the ISR manager will need to verify:
    - The classification level of imagery services that he can make available to the user – some sensor's data cannot be declassified to a level that is widely "disseminateable." The match between the user's clearance and the services available to collect the information will be "matched" via the user profile and the service's profile of available output and distribution formats available.
    - The format and size of the file the user can receive must be accommodated. Some imagery files can be large – the capabilities of the end user's device, as well as the "pipe" connecting it to the network must be taken into consideration. Once again, the match between these criteria will be accomplished through pairing of the user's profile with the service's output and distribution format availability profile.

    - Both of these capabilities will need some sort of service and/or hardware/software to accomplish this pairing task (user to services available).
- The imagery service demonstrated here has a "man in the loop," but could easily be automated.
- Taking the extreme case, and assuming a construct along these lines is adopted DoD-wide, one could envision the global information grid (GIG) becoming the "mother of all COIs." It encompasses all Joint capabilities' COIs, and information can be accessed via the mechanization of the profile-based publish/subscribe mechanism. Functionally, this holds true throughout all echelons, and via the collaboration capability, will provide the mechanism for self-synchronization throughout all echelons of command. This eventually may make orders preparation an after-the-fact historical document, rather than a tasking instrument.

CONCLUSION

In attempting to provide a concept of operations describing NCW in language "understandable to to the rest of us," I've attempted to go a level beyond the platitudes normally spoken during discussions about NCW, and provide a concrete example of how NCW *could* work. As a point of departure for discussing NCW-related issues, I believe it provides a common framework for discussing issues related to NCW, and provides the core around which further documentation can be developed to make NCW a reality. In the endgame, NCW isn't about "all information, everywhere, all the time" – it's about being able to find the most current and appropriate information in a timely fashion and provide it to the end user in a format he can use; then and only then can we hope to achieve the vision of self synchronization required to keep one step ahead of the enemy, which, in the endgame is what it's all about.

"Buzzword Bingo" – a Short List of NCW-related Terms

Understanding the "lingo" is half the battle -- attached are NCW terms of reference. If there's a term used in the article or in the definitions below that is unfamiliar to you, it is likely listed here; terms are in alphabetical order.

Catalog: contains indexed information allowing for referencing all information available in the COI, to include subordinate COIs

- Catalogs will use XML (eXtensible Markup Language) to describe the contents of information available to the COI (i.e., metadata)
- Schema for multi-COI catalog distribution is required for catalog alignment and update
- **Key point about Catalogs**: despite what you've heard about NCW… NCW *does not* mean "all the data is everywhere, all the time" – it's about a schema for cataloging, accessing, and subscribing to tailored information

Collaboration: use of online tools to involve subject matter experts in the decision-making process that aren't collocated. DCTS (Defense Collaborative Tool Suite) trying to "bridge the gap" between vendor tools

Community of Interest (COI): the collection of people that are concerned with the exchange of information in some subject area

- COIs can be organized around any group of entities with a common interest, or in the case of the military, common mission
- COIs are not mutually exclusive; one can be a member of several COIs at the same time
- Assumption: COIs will provide the groupings by which Service-Oriented Architectures are designed
- Source: **A Community of Interest Approach to Data Interoperability,** Scott A. Renner, Ph.D. http://www.mitre.org/work/tech_papers/tech_papers_01/renner_community/index.html)

Defense Collaboration Tool Suite (DCTS): DCTS is a flexible, integrated set of applications providing interoperable, synchronous and asynchronous collaboration capability to the Department of Defense's (DoD) Combatant Commands, the military services and DoD agencies. The DCTS Program identifies, fields and sustains a dynamic set of evolving standard collaboration tools that bridge between DoD and the Intelligence Community. These tools enhance simultaneous, ad hoc crisis and deliberate continuous operational action planning (vertically and horizontally) across operational theaters and other domains that provide operational units and defense organizations simultaneous access to real-time operational, tactical, and administrative information (http://www.disa.mil/pao/fs/dcts2.html).

Horizontal Fusion: means and tools enabling the smart pull of information via machine-to-machine interfaces direct from the source of the information, in order that the information may be fused with other data to provide actionable information for the warfighter.

Joint Command and Control Capability (JC2): used to be GCCS…
http://diicoe.disa.mil/coe/aog_twg/twg/coptwg/jc2ord.ppt

Metadata: "data about data." Information by which artifacts are cataloged and stored.
DISA Vision on metadata includes information about each artifact created, stored in 4 catalogs based on a telephone book paradigm (Source: Briefing -- "*Market-Driven Data Management,"* Dawn Meyerriecks, Chief Technology Officer, Defense Information Systems Agency):

- White Pages: who created the information
- Yellow Pages: what the information is
- Brown Pages: how data stored (information about formatting rules associated with the information – called "ontology's" by overeducated software engineer types). Think: internal formatting of Microsoft Word vs. Lotus Notes – it's the rules by which an application renders and displays information
- Green Pages: security/classification requirements (think "behind the green door")

Network Centric Warfare (NCW): …an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. In essence, NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace… (Source: **Network Centric Warfare,** Alberts, Garstka, and Stein, CCRP)

Portal: A site featuring a suite of commonly used services, serving as a starting point and frequent gateway to the Web (Web portal) or a niche topic (vertical portal). Civilian web portal services often include a search engine or directory, news, email, stock quotes, maps, forums, chat, shopping, and options for customization. Portals for NCW are generally a specialized type of portal called an **Enterprise Knowledge Portal**, which is an enhanced Portal that:

- Is goal-directed toward knowledge production, knowledge integration, and knowledge management
- Focuses upon, provides, produces and manages information about the validity of the information it supplies
- Provides information about your business and meta-information about the degree to which you can rely on that information
- Distinguishes knowledge from mere information
- Provides a facility for producing knowledge from information
- Orients one toward producing and integrating knowledge rather than information
- Sources:
  - http://www.marketingterms.com/dictionary/portal/
  - Implementing Enterprise Knowledge Portals http://www.dkms.com/ekpcons.htm

Publish and Subscribe: a process by which data is distributed inter- and intra-COI

- "Smart," filtered push and pull of information is based on filters selected by the user during subscription process. "Push and pull" – the information can either be provided to the user upon creation (smart push), or the user can be notified that the information is available, and pull it at his leisure (smart pull)
- "Civilian world" examples include automated stock ticker, news, and weather reporting programs:
  - Pointcast, Infogate (stocks)
  - E-Mail News Servers
  - WeatherBug
- **Publish:**
  - **Advertise**: make information available for consumption. Includes development of all catalog metadata
  - **Distribute**: to service the subscription list
  - **Post**: to make available information on the status of an asset (location, systems/sensors' status, fuel status, etc.), indicates new information is available for:
    - Advertisement
    - Distribution
    - Aggregation/Analysis
- **Subscribe**:
  - Webster's:
    - To enter one's name for a publication or service
    - To receive a periodical or service regularly on order

- For NCW: to register to be the recipient of a distribution of information upon its creation and subsequent updates
  - Specification of the type of information one wishes to receive
  - Subscription Types:
    - New Information Available: provides link to information instead of the actual information - enables "Smart Pull" of information when user is ready to use it
    - Information Delivery Upon Creation: deliver information upon creation by either the creator of the information, or an intermediate distributor

Security Assertion Markup Language (SAML): is "an XML-based framework for exchanging security information. (http://xml.coverpages.org/saml.html)

Service: the execution of a capability by one entity for use by others

Service-Oriented/Service-Based Architectures: (informal definition) business-to-business, web-based applications; usually rely on a great degree of trust between service provider and user (http://www.w3.org/TR/2004/NOTE-ws-arch-20040211/#service_oriented_architecture)

Simple Object Access Protocol (SOAP): Version 1.2 (SOAP) is a lightweight protocol intended for exchanging structured information in a decentralized, distributed environment. It uses XML technologies to define an extensible messaging framework providing a message construct that can be exchanged over a variety of underlying protocols. The framework has been designed to be independent of any particular programming model and other implementation specific semantics (http://www.w3.org/TR/2003/REC-soap12-part1-20030624/#intro)

Swarming: "useful self-organization of multiple entities through local interactions"

- "Stigmergic"
  - From the Greek words for sign and action
  - Example: ants and bees use pheromones initiate actions in the group
- Rules-based:
  - Polyvalent: all members of the potential swarm have the same ruleset and similar skills; swarm uses signals to unify action
  - Specialized:
    - Members come in different configurations
    - Based on signals received from other group members, members adapt community behavior based on rulesets; specific members take on duties matched to their skillset
- Applications:
  - Animals: Foraging optimization, nest defense
  - Military:
    - "Smart Mobs" employing self-synchronization (Chechnya, Somalia)
    - Decision aids for self-synchronization
- Sources -- White Papers for Swarming Network Enabled C4ISR Conference 13-14 January 2003, McLean, VA:
  - "Making Swarming Happen," Dr. Van Parunak, Altarum
  - "Military History of Swarming," Mr. Sean Edwards, NGIC
  - "Swarming Intelligence," by Dr. Eric Bonabeau, Icosystem Corporation

Task, Post, Process, Use (TPPU):

- Basic tenet of NCW, based on the concept that consumers of information are smarter than their sources about what is operationally needed "NOW"
- Term derived from Intel TPED (Task, Process, Exploit, and Disseminate), which was often was criticized by operations for providing "cooked" information too late for operational use
- Implications:
  - Information derived from collections will be posted for community use prior to processing and exploitation via use of "Smart Pull" technologies (i.e., Publish/Subscribe)

- Enables community users to make use of “raw information” in a more timely fashion for their particular operational application
- Source: TPPU, the New Paradigm (DISA GIG NCES Website) http://ges.dod.mil/about/tppu.htm

UDDI (Universal Description, Discovery and Integration)

- A "meta service" for locating web services by enabling robust queries against rich metadata
- **http://www.uddi.org/**

Virtual Private Networks (VPN):

- Enables multiple “virtual” networks to exist over common media
- Enables distant users to appear on the network as if they were “local users”
- Example: company intranets

Web Services Description Language (WSDL – pronounced “whiz-dill”): an XML-based language for describing Web services and how to access them (source: http://www.w3schools.com/wsdl/wsdl_intro.asp)

XML: e**X**tensible **M**arkup **L**anguage

- Tag-based, hierarchical markup language for description of data and its relationships
- Contrasted with HTML (HyperText Markup Language), another markup language:
  - HTML specified by typing “http” [HyperText Transfer Protocol] in web addresses)
  - Fixed-meaning tags embedded in document (in your web browser, hit View => Source to see the tags in the document)
- Differs from HTML in that the user can define the tags which are used to describe data in a page (in HTML, the tags are fixed)
- Tags “standardized” in communities by definition of Namespaces
- DoD Namespaces being managed by DISA
  - XML Registry: http://diides.ncr.disa.mil/xmlreg/user/information.cfm
  - Namespaces have been “binned” by predefined COIs:
    - Command and Control
    - Intelligence
    - etc.
- Standard format for XML is unicode, which in most implementations takes 16 bits per character (ASCII takes 7 or 8, depending upon implementation)
  - Possible implications with size of data after “XML-izing”
  - Possibly mitigated with data compression techniques

References:

"Net Centric Enterprise Services – What Problem are we Trying to Solve?" Dawn Meyerriecks CTO, DISA, Military Information Technology, online edition, Volume 7, Issue 3, March 2003 http://ges.dod.mil/articles/netcentric.htm

Briefing: "NCES Net Centric Enterprise Services," Rob Vietmeyer/DISA APC

A Community of Interest Approach to Data Interoperability
Scott A. Renner, Ph.D., Member, AFCEA
The MITRE Corporation
http://www.mitre.org/support/papers/tech_papers_01/renner_community/renner_community.pdf

Understanding Information Age Warfare
David S. Alberts, John J Garstka, et. al.
CCRP, August 2001

DISA Briefing: Market-Driven Data Management
Dawn Meyerriecks
Chief Technology Officer, DISA
10 Apr 2002

Understanding Information Age Warfare
David S. Alberts, John J Garstka, et. al.
CCRP, August 2001

Joint Staff J-6 Brief: ***XIII Joint Tactical Communications Summit,*** Robert M. Shea, LtGen, USMC, Joint Staff J-6, 05Feb04
http://www.envoke.us/
http://www.asolutions.com/movies/CollaborationPres512.wmv