Net-Centric Conversations: The Enterprise Unit of Work

Harvey Reed and COL Fred Stein (Ret.)
MITRE

Net-centric warfare and Net-Centric Operations (NCO) require systems and systems of systems to be increasingly agile. The challenge is how to design and modify such agile systems. This article suggests that the concept of Net-Centric Conversations (NCC) can be used to increase and track the agility of systems, in support of both humans and machines. An NCC is an operational mission thread or business process expressed, according to a set of five organizing principles. These principles support a formal description of the people, machines, weapons, and sensors, and their cooperative relationship that produces a net-centric capability. The term conversation *is deliberately used to capture the essence of an NCC's ability to describe the interactions between the participants, both humans and machines, involved in the mission thread or business process. Each NCC is version controlled, ensuring that all participants are aware of relevant changes in others, allowing continuous configuration management and build-up of trust between them.*

This article discusses a practical and innovative means to create and manage net-centric capabilities that span systems and people. The intended audience includes both acquisition and operational leaders. The concepts are most germane to those who have tried to field Web services or publish/subscribe services and who have tried to integrate these services with other likewise programs. There is almost a universal frustration with the current program-centric approach to constructing net-centric capabilities that span systems and people; this article proposes an alternative.

Net-centric warfare and NCO are based on the existence of a highly connected force capable of leveraging the interdependent relationships among sensors, shooters, and decision makers, all enabled by information technology. Net-centric capabilities (such as new *kill* or *supply chains*[1]) are generated by relating multiple weapons, sensors, and people together, either permanently or temporarily. These net-centric capabilities require supporting complex relationships. Traditional bilateral interface exchanges such as Interface Exchange Requirements and Interface Control Documents (ICD) are insufficient to describe and manage complex net-centric capabilities. Since the Department of Defense (DoD) has no formal mechanism to describe and manage such relationships, it is difficult to maintain trust among participants, which slows adoption of NCO.

To construct the kind of net-centric capabilities discussed, the primary focus is on creating and managing relationships among the participants (sensors, shooters, decision makers, supporting machines, and people) who use the network to exchange messages. We are not talking about the network itself (routers, bridges, pipes, etc.), except for the intersection cases where a firewall or proxy would interfere with the exchange of messages. This distinction is important because the network itself should be largely unconstrained in how it delivers services. We will assume the network service is highly available and has the ability to deliver messages.

> *"In a multilateral NCC, many program offices will contribute services, and the impact analysis must alert all potentially affected program offices of a pending change that the group needs to discuss."*

Further, individual systems with Web and messaging technologies such as enterprise service bus (ESB) do not construct net-centric capabilities in and of themselves. They provide connection mechanisms; the hard part is describing, recording, and managing the relationships you want to create.

Figure 1 highlights the difficulty of constructing a net-centric capability on top of a network using bilateral techniques to construct and manage relationships among participants. Three stovepipe systems are individually exposing services (such as Web services, or publish/subscribe services) to exchange messages. The messages can contain targeting information from a Command and Control system or perhaps logistics, as well as personnel information from an operations support system. The messages can be exchanged with a variety of techniques including publish/subscribe, and/or Web services.

The desired end-state capability spans all the participants, including the services and end-users. Current interface agreements are bilateral, forcing us to use at least three agreements in this simple example. Further, there will be multiple negotiations with security officers for each of the systems since the messages exchanged will likely be passing through firewalls, proxies, etc.

Once the capability is constructed, it is difficult, if not impossible, to change because there is no focal point for change control or impact analysis. Adding to this, there are too many separate agreements to change in a coordinated fashion.

The alternative to creating and managing separate bilateral agreements is to create a single multilateral agreement, as shown in Figure 2. This centralizes change impact analysis and aids in coordinating change. Change is necessary to implement agility to respond to unanticipated events. It is only with a single multilateral agreement and correspond-

ing agility metrics that agility can be measured and improved over time.

Publish-01 is the name of the net-centric conversation that binds all the participants listed in the legend.

NCC: The Definition

An NCC is a persistent, multi-party agreement describing the relationships between sensors, shooters, decision makers, and other participants that create a net-centric capability. This agreement is ideally stored and managed in an NCC discovery service as an extension to the metadata environment for the enterprise. NCCs are supported by the following five organizing principles.

NCC Principle 1

An NCC is described, registered, and discoverable. NCC is a binding layer (see Figure 3) for the messages and mission services (warfighter and business capability) that, in turn, use enterprise services. The NCC describes critical roles for people, support doctrines, and procedures; it is entered into an NCC registry so that impact analyses can examine any proposed changes. This impact analysis must support both low-level and high-level changes. In a multilateral NCC, many program offices will contribute services, and the impact analysis must alert all potentially affected program offices of a pending change that the group needs to discuss.

Stability of message structures are critical to the stability of NCCs. Individual mission services can change their implementation with no impact on participants; however, the same cannot be said of message structure. Future message structures will be defined as extended mark-up language (XML) schemas whose vocabulary will be well defined and explained by community of interest (COI) data panels. The value of XML is that it is flexible and can allow extensions, but changing the core structure or the vocabulary itself will have far-reaching effects.

NCC Principle 2

An NCC is described by message exchanges of participants. An NCC groups machines and users in a transitive, multilateral agreement to produce a net-centric capability. As shown in the NCO examples and in the notional scenario in Figure 4 (see page 20), the NCC is defined by the exchange of messages; this information is what is recorded in the NCC's entry in the NCC registry, as well as supporting Concept of Operations (CONOPS) and other ancillary materials to aid in the understanding and measure-

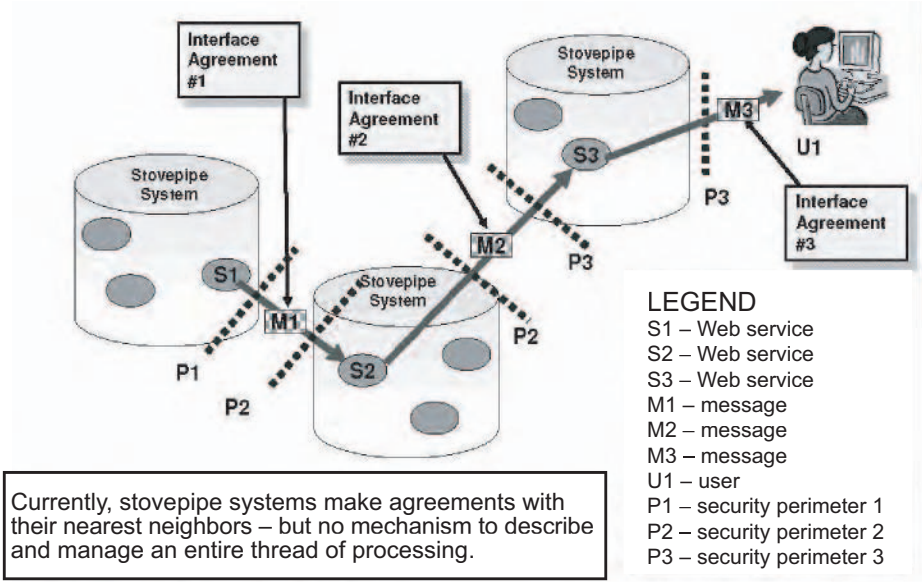


Figure 1: *Stovepipe Systems – Separate Agreements*

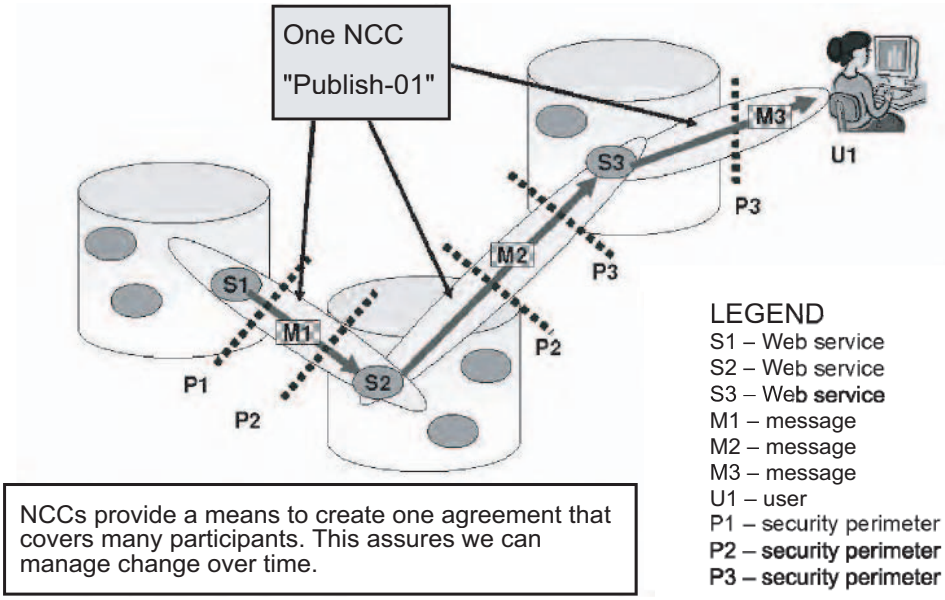


Figure 2: *NCCs – Single Agreement*

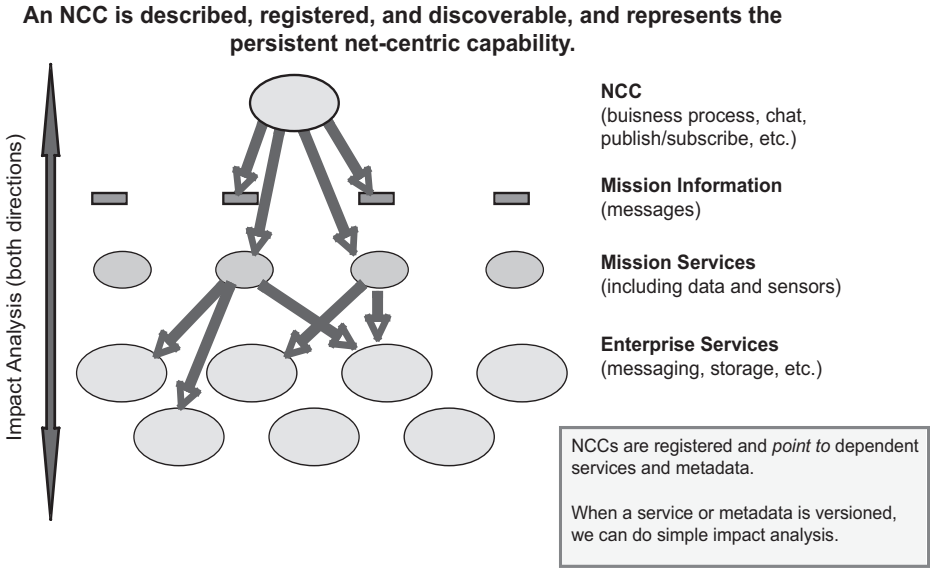
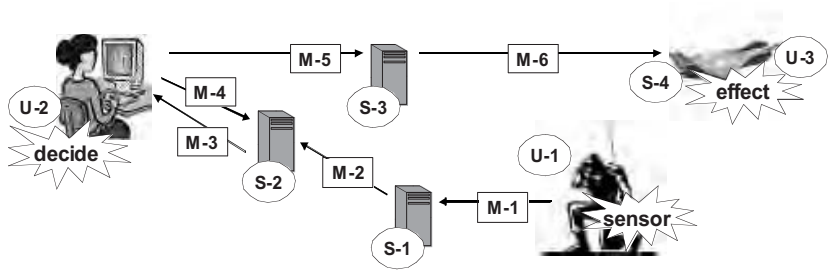


Figure 3: *NCC Principle 1*

An NCC has both human and machines as participants and is completely described by the set of possible message exchanges between them.



NCC Name	Users	Systems	Messages	CONOPS and Doctrine	Mission Effectiveness KPIs
Laser -target -01	U-1, U -2, U-3	S-1, S-2, S-3, S-4	M-1, M -2, M-3, M-4, M -5, M-6	SOF	1. Ave time to target 2. Ave accuracy

Figure 4: *NCC Principle 2*

An NCC has an agility profile derived from the agility metrics of the participants and messages.

(NOTIONAL)

Participant Type	Participant Name	Minimum time to develop/train	Organization	Minimum time to reconfigure
User	U-1	Train=10 days	AETC	n/a
Service	S-1	42 days	Contractor -1	n/a
Service	S-2	67 days	Contractor -2	13 days
Service	S-3	83 days	Contractor -2	5 days
Message	M-1	120 days	COI -1	n/a
Message	M-2	160 days	COI -1	n/a
Message	M-3	200 days	COI -2	n/a
Perimeter	P-1	n/a	AFNOSC	Firewall=90 days
Perimeter	P-2	n/a	DISA	Firewall=60 days
Perimeter	P-3	n/a	DISA	Firewall=45 days

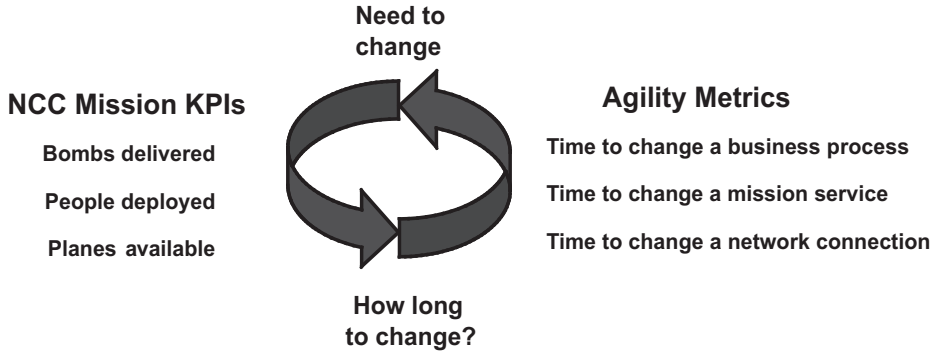
AETC – Air Education and Training Command
COI – Community of Interest
AFNOSC – Air Force Nodal Operations Service Center
DISA – Defense Information System Agenc

Figure 5: *NCC Principle 4*

ment of the NCC. In Figure 4, we see a sample entry in an NCC registry. Each reference of a participant points to its entry in its own registry. The NCC registry then becomes a new, fifth type of discovery that consists of a set of relationships between participants but does not describe any individual participants in detail.

Figure 6: *NCC Principle 5*

Portfolio management of NCCs reduces the complexity of the enterprise, and forms the basis of value-based evolution of the enterprise.



NCC Principle 3

An NCC is associated with Key Performance Indicators (KPIs). Each NCC is associated with a set of one or more KPIs which are expressed in terms of warfighter and/or business-level measurements, as appropriate. A portfolio manager can assess the contribution of the NCC to the value of the overall portfolio. Further, if the portfolio manager wants to improve the NCC value (KPI), it can be done in an objective manner and balanced against the cost of changing the NCC, as revealed by its agility profile (see Principle 4). The NCC KPIs will be derived from a combination of human/ machine observations (e.g., time to target, target assessment), as well as lower level information technology infrastructure measurements (time for certain messages to arrive or be dispatched).

NCC Principle 4

An NCC has an agility profile. One of the metrics required for managing *NCCs is the minimum time to change (including configuration)* associated with participants. These individual measurements (see Figure 5) are summarized into the minimum time to change any NCC and depend on the develop/deploy/configure processes used by each participant's organization. With quantification of agility, we can focus policy and resources on high-priority slow spots. NCC agility metrics will, for the first time, give us a numerical view of the level of agility in the enterprise, which is a key performance metric for DoD transformation.

NCC Principle 5

Portfolio Management of NCCs reduces complexity of the enterprise. NCCs are portfolio managed with KPI performance metrics balanced against agility metrics, as shown in Figure 6. This additional transformation tool helps to rationalize the process of adding net-centric capability to the enterprise. This portfolio management consists of NCCs that express multilateral relationships among participants. It assumes the participants can use network connections and services that are managed separately.

- Leadership (military and civilian) can understand the capability of an NCC because it is described in warfighter and/or business terms.
- Leadership can understand the per-

formance of an NCC because the performance is measured in warfighter/business terms.
- Leadership can understand the minimum time to change an NCC because there is an agility profile associated with it.
- Leadership can balance the need to improve KPIs against anticipated agility costs in an objective manner.

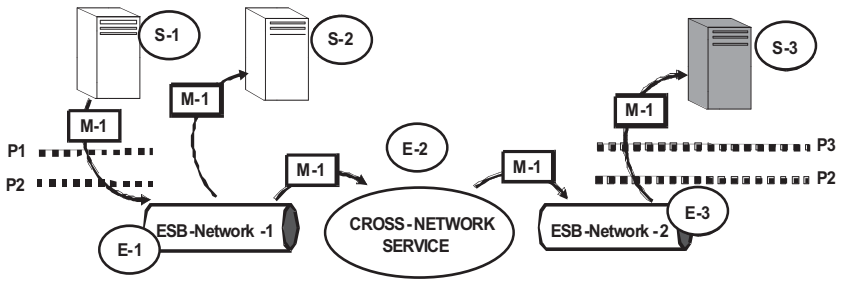
Leadership can also understand how NCCs relate to each other because NCCs can be assembled to yield compound NCCs. The set of all NCCs and their relationships to each other represent the *as-built* architecture of the enterprise, expressed in capability terms. This will focus leadership attention on integrated capability transformation and away from isolated systems or particular technologies.

Example From Global Combat Support System – Air Force (GCSS-AF)

The GCSS-AF supplies shared resources such as computing infrastructure for Air Force Operations Support applications and services. GCSS-AF provides application, hosting, data, integration, and security services, as well as the Air Force Portal. GCSS-AF integration services include an ESB that allows applications and services to exchange messages. GCSS-AF is currently developing its first NCC. Figure 7 shows how GCSS-AF assembles mission and infrastructure services into NCCs to deliver a net-centric publish/subscribe capability.

Figure 7 shows a notional example of a simple personnel notification: a key enabler of net-centric warfare that helps share awareness among participants and increases self-synchronization. Publishing Service S-1 (personnel) sends a notification message to the ESB E-1 service on the ESB Network-1 side of GCSS-AF. The notification takes the form of a publish message, M-1. The ESB E-1 then pushes Message M-1 to Subscribing Service S-2 (force readiness) on the ESB Network-1 side and also to Subscribing Service S-3 (warfighter) on the ESB Network-2 side via the cross-network service E-2 (semi-automated air gap).

Even this very simple example (one publisher, two subscribers) involves 10 participants: three services, two ESBs (ESB network-1 and ESB network-2), the cross-domain service, the message payload schema/semantics, and three security perimeters. If any one of the participants must change, each of the remaining participants must be notified beforehand. Each type of change must be coordinated and must be associated with different agility metrics. Table 1 continues the notional example.



NCC Name	Users	Systems and Services	Messages	Security Perimeters	CONOPS and Doctrine	Mission Effectivess KPIs
Notify - 01	none	S-1 (personnel) S-2 (force readiness combat support) S-3 (force readiness warfighter) E-1 (ESB) E-2 (ESB) E-3 (ESB)	M-1 (airman status change)	P1 (personnel security) P2 (GCSS - AF security) P3 (warfighter security)	Alert Airman status change	1. Average time to deliver alert from personnel to warfighter 2. Percent delivered from personnel to warfighter

Figure 7: *GCSS-AF Notification Using Enterprise Services*

These agility metrics come into play when evaluating proposed NCC changes to determine the shortest amount of time needed to make a version change. We can balance the value of the change against cost and time.

Summary

Beyond creating NCCs in a large environment such as GCSS-AF, it is an easy extension to envision NCCs that span environments, such as GCSS-AF to GCSS-Marine (GCSS-M). The NCC would still be recorded as a single entity in one NCC registry. One of the participants could be a GCSS-M service, and the NCC entry in the NCC registry would point to the service description in the GCSS-M service registry, as well as service descriptions in GCSS-AF. The message exchanges would likely be enabled by inter-ESB connections between the two environments. Federating ESB connections is beyond the scope of this article, but is actively explored by current GCSS-AF activities.

Additionally, NCCs will ultimately be a collaboration of the acquisition community and operational users in the field. We must be able to support both institutional pieces of an NCC, as well as be able to substitute devices on the tips of the NCC in the field by leveraging configuration and/or lightweight development.

Net-Centric Warfare and NCOs are taking place every day in support of the Global War on Terrorism. The United States and its allies in NATO continue to leverage Information Age technology to support missions worldwide. As more systems are deployed and the need for enterprise level coordination and information exchange increases, the concept of NCCs can provide a development and maintenance advantage.

NCCs do not preclude the use of Web services that are intended to be used by *everybody*, such as weather. There will continue to be a need for Web services that are put in the field,

Table 1: *Sample NCC Agility Metrics*

The ESB needs to be configured when new subscribers are added – no impact to existing subscribers, but the publisher must be notified due to security policy.	1 day
SOA lets us easily substitute services as long as interfaces are maintained – no impact to other participants.	5 days
Subscribing services need to change if message payload semantics change – potential large impact – notification and analysis required.	180 days
Cross-domain services if implemented as a guard need to change filters if message semantics change – changes in guard filters require a lengthy accreditation process.	6 months to 1 year

used relatively anonymous in a bilateral fashion (user/Web service), and will not change much over time. NCCs are intended for cases where we want repeatable, evolvable multilateral capabilities. There is no choice but to record them and manage them.

NCC's organizing principles enable us to build net-centric capabilities from relationships among new and existing information systems and users. These capabilities are measured with KPIs. They also allow us to maintain version control across all participants in an NCC and to track agility metrics, which quantify the minimum time needed to change individual NCC capabilities and the enterprise as a whole. Understanding the overall agility of the enterprise is critical to a successful transformation of the enterprise to net-centricity.◆

Note

1. A kill or supply chain links participants together in a common activity. For example, in a kill chain, we can have a targeter, an air space controller, and a pilot all working together to affect a target. In a supply chain we have the product company, distributor, shipping company, and retail stores working together to bring products to the consumer.

About the Authors

Harvey Reed joined MITRE in 2004. He is currently the chief engineer for the GCSS-AF. He led the delivery for the first ESB in the Air Force, delivered in March 2005. He is currently leading the delivery for the first Metadata Environment in the Air Force, to be delivered in the Summer of 2007. Prior to joining MITRE, Reed was a product manager at Sonic Software for business process products, as well as a voting member of the OASIS Web Services Business Process Executive Language Technical Committee. He has a bachelor's degree from Purdue University in pure math and computer science, and a master's degree from Georgia Tech University in computer and information science.

MITRE
45 Arnold ST
MS 1600H
HAFB, MA 01731
Phone: (781) 377-0823
Fax: (781) 377-1423
E-mail: hreed@mitre.org

Fred Stein is a retired U.S. Army Colonel. Currently, he is a MITRE senior engineer for Network Centric Warfare. His position and location at Ft. Hood, Texas within the Central Test and Support Facility provides him the opportunity to interface directly with the Army as it digitizes its force and moves toward the Future Combat Systems. He also serves as a member of the the Swedish National Advisor Board on Network Based Defense, advisor to the Office of Secretary of Defense Office of Force Transformation, and is an Assistant Professor at the Army War Collage. Stein has a bachelor's of science in industrial management from Georgia Technical Institute and a master's of science in operations research (business) from Boston University.

MITRE
P.O. Box 10237
Killeen, TX 76547
Phone: (254) 702-0815
Fax: (703) 564-9848
E-mail: fstein@mitre.org