

Modeling and Simulation Integration with Network-Centric Command and Control Architectures

John J. Daly
Booze Allen Hamilton
Suite 1100
1725 Jefferson Davis Highway
Arlington, VA 22202
(703) 412-7432
daly_john@bah.com

Dr. Andreas Tolk
Virginia Modeling Analysis & Simulation Center
Old Dominion University
Norfolk, VA 23529
(757) 686 - 6203
atolk@odu.edu

Keywords:

Net-Centric Warfare, Network Centric Operations and Warfare (NCOW), M&S-to-C4ISR Interoperability, Global Information Grid (GIG), GIG Enterprise Services (GES), Joint Command and Control System (JC2)

ABSTRACT: *Network Centric Command and Control operations postulate that the more information we can collect, create, and share about the adversary, the operational environment, our capabilities, readiness, and logistics, the more we can focus our capabilities to produce desired effects with less risk of unintended consequences and more efficient expenditure of national resources. The critical role of the Global Information Grid (GIG) Enterprise Services (GES) in an integrated, net-centric, Joint Command, and Control System (JC2) architecture can not be understated. JC2 requires new capabilities and C4I architectures will require transformation from hierarchical, distributed, broadcast systems based on the tactical data systems of the 1970's.*

This migration to an information sharing and dissemination system will need to include both a hierarchical (to accommodate military C2 doctrinal functions) and a peer to peer ability to share and access information and functionality between all levels in the Command and Control system. This new capability is required to enable sharing of unprocessed or uncorrelated raw data with selected users on demand, and allow distributed the functionality of advanced collaborative planning, coordination and decision support applications. Further, with this advanced information flow and accessibility, intrinsic C4 applications to enable "sense making" of information overload and for tailoring a C4 node to a specific purpose or role become apparent.

This new role for C4I requires applications traditionally found in the Modeling and Simulation community of interest. They must be integrated into real-time Network Centric C4I and will perform an important function in the enhanced capabilities of the JC2 Joint C4I system of the future. This paper discusses classes of M&S based C4I applications that support the net-centric requirements of the JC2, how the GES will include intrinsic Modeling and Simulations services to support such applications, and the parallel technologies that can benefit both the C4I and M&S communities of interest.

1 Introduction

"Possibly the single-most transforming thing in our forces will not be a weapons system, but a set of interconnections and a substantially enhanced capability because of that awareness." —Secretary of Defense Donald Rumsfeld, August 9, 2001.

Joint Vision 2020 clearly notes that "Command and Control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission." A Command and Control Computer system and its associated data links and communications infrastructure make up the Command, Control, Communications, Computers and Intelligence (C4I) system and are part of the equipment that supports the commander in performing the Command and Control (C2) function.

Importantly, this C4I equipment is designed, manufactured, and operationally deployed to become part of a C2 system based on military doctrine and operated by military personnel. As military doctrine changes, so must the tools to implement that doctrine in the C2 process, and conversely as C4I tools improve, the C2 doctrine will change to exploit their capabilities. As we have migrated from the mainframe and client-server to net-enabled architectures, military C2 doctrine has also migrated from a rigid hierarchical information model, to a more rapid horizontal integration and fusion of information to all echelons in the C2 structure. This has clear advantages in achieving Information Superiority in the battlespace and is the genesis of the concept of Network Centric Command and Control.

Network Centric Command and Control operations postulate that the more information we can collect, create, and share about the adversary, the operational environment, our capabilities, readiness, and logistics, the more we can focus our capabilities to produce desired effects with less risk of unintended consequences. Situational awareness knowledge becomes a hedge against uncertainty, allowing deployment of more precisely tailored capabilities and enabling increased speed and degree of decisiveness of action. This requires timely access to this knowledge by the decision maker, and the ability to tailor the knowledge in an intuitive man-understandable format for rapid cognition.

C4I systems have evolved from being “message generators driven by databases” via their inception as essentially electronic “maps” displaying geographical position of known units and platforms (“tracks”), including the concept of a “Common Operating Picture” (COP), and information systems organized based on the hierarchical military “Chain of Command” utilized by the users. The geospatial integration of information into a map format is a natural, intuitive way for decision makers to see a summary of information with the all-important element of force disposition preserved in the display. That they would obtain that information hierarchically is natural, as “track” (force positions over time) information is correlated and processed as it moves up the hierarchy from sensor to decision-maker. Other information that the decision-maker might use, such as intelligence and logistics information traditionally has been provided via other dedicated systems, or directly as paper messages, voice reports, and other means. There has been a growth of new forms of information for that military decision-maker that do not readily follow the hierarchical chain of command, and that we now wish

to geographically insert into that electronic map as integrated geospatial information. There also has been a desire to integrate battlefield information systems into one system vs. multiple “stovepipes” for various information needs.

Alternate methods of integrating information other than traditional tracks into a “Common Operational Picture” (COP), is possible by utilizing C4I system applications to present synthetic views of that new information. This can simply be the geospatial presentation of information in a hyper-link format not usually shown on a typical track-centric “electronic map” based C4 system. This is a tremendous advance over standalone database queries, by giving the information a geographical context and selection criteria. Other adaptive views can enable cogent situational awareness of information normally beyond human cognition via advanced processing of that raw data. This occurs much the same way that modern radar presents synthetic video on its display vice raw, unprocessed radar return video.

All of these approaches require the dissemination and decision maker cognition of more and more data and information. That data needs to flow both vertically, up and down the Military Chain of Command as well as horizontally from individual elements in the chain of command, and other users or nodes that might be outside the traditional C4I domain. The traditional method of hierarchical information dissemination from the data collector to data subscriber has to migrate to a new concept, where all users have all information required whenever and wherever. This requirement can only be satisfied by applying new data dissemination principles which are much more open and flexible.

A concept of Network Centric Warfare (NCW) has evolved to meet the challenges that modern information centric warfare provides. Computer, networking, and sensor technology is now capable (at least in part) in piercing the impenetrable “Fog of War” [1] that Clausewitz postulated almost 200 years ago.

2 Network Centric Operations and Warfare

The term Network Centric Operations describes a broad class of approaches to military operations that are enabled by the networking of the force. When these military operations take place in the context of warfare, the term Network Centric Operations and Warfare (NCOW) is applicable.

Network Centric Operations provide a force with access to a new, previously unreachable region of the

information domain. The ability to operate in this region provides the Warfighter with a new type of information advantage leading to the desired objective of Command and Control advantage. This advantage is enabled by dramatic improvements in information sharing made possible via networking. With this information advantage, a warfighting force can achieve dramatically improved shared situational awareness and knowledge.

In this context, the ability to achieve a heightened state of shared situational awareness and knowledge among all elements a force, including allied and coalition partners, is increasingly viewed as a cornerstone of C4I transformation. Emerging evidence from recent military operations and a broad range of experimentation supports the relationship between shared situational awareness and knowledge enabled by NCW concepts and increased combat power, see [2].

According to Alberts et al. [3], NCW concepts can be understood by focusing on the relationships in warfare that take place simultaneously in and among the physical, the information, and the cognitive domains.

- **Physical Domain:** The physical domain is the traditional domain of warfare. It is where strike, protect, and maneuver take place across the ground, sea, air, and space environments. It is the domain where physical platforms and the communications networks that connect them reside. Comparatively, the elements of this domain are the easiest to measure, and consequently, combat power has traditionally been measured primarily in this domain.
- **Information Domain:** The information domain is the domain where information lives. It is the domain where information is created, manipulated, and shared. It is the domain that facilitates the communication of information among Warfighters. It is where the command and control of modern military forces is communicated, where commander's intent is conveyed. Consequently, increasingly the information domain must be protected and defended to enable a force to generate combat power in the face of offensive actions taken by an adversary.
- **Cognitive Domain:** The cognitive domain is the domain of the mind of the Warfighter and the Warfighter's supporting populace. Many battles and wars are won or lost in the cognitive domain. The intangibles of leadership, morale, unit cohesion, level of training and experience, situational awareness, and public opinion are

elements of this domain. This is the domain where commander's intent, doctrine, tactics, techniques, and procedures reside. The key attributes of the cognitive domain have remained relatively constant since Sun Tzu wrote The Art of War.

A warfighting force that can conduct Network Centric Operations needs to have the following attributes and capabilities:

- **Physical Domain:** All elements of the force are robustly networked achieving secure and seamless connectivity.
- **Information Domain:** The force has the capability to collect, share, access, collaborate, analyze, and protect information, achieving an information advantage over an adversary.
- **Cognitive Domain:** The force has the capability to develop shared knowledge of commanders' intent, share high-quality situational awareness, and self-synchronize its operations

The central hypothesis of NCW is that a force with these capabilities can increase combat power by: better synchronizing effects in the Battlespace, achieving greater speed of command, and increasing lethality, survivability, and responsiveness, see [3].

The concept of Network Centric Operations and Warfare (NCOW) is a realization that modern warfighting efforts are a synergy of command and control, enterprise business operations, both hierarchical and asymmetric networking, and advanced cognitive software applications. They impact all levels of military activity from the tactical to the strategic. In order to successfully conduct warfare the Commander must simultaneously work in the Physical, Information, and Cognitive domains maintaining optimum situational awareness in all three. This is the challenge of modern Command and Control in general, and in particular a challenge for the supporting C4I systems. The information domain must bridge the gap between the physical and the cognitive domain as much as possible.

3 Global Information Grid

An underlying information technology infrastructure must support all layers of decision making, all level within the hierarchy, and all participants in the Command and Control process with the necessary information and the necessary applications (including collaboration tools and decision support systems) in a parallel, emerging manner.

3.1 Vision for the GIG

The means for accomplishing this in the U.S. Department of Defense (DoD) is the Global Information Grid (GIG). A globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to Warfighters, policy makers, and support personnel.

The GIG is a key enabler of NCOW and is essential for information and decision superiority. It will enable C4I integration of joint forces, improve interoperability of systems, and increase optimization of bandwidth capacity thereby dramatically improving warfighting capabilities. The GIG will enhance operational capabilities while providing a common environment for conventional and nuclear Command and Control (C2), combat support, combat service support, intelligence, and business functions. In particular, the GIG will support:

- Ability to operate with reduced forces at high operational tempos where dynamic planning and redirection of assets is the norm.
- Delivery of information concerning targets, movement of forces, condition of equipment, levels of supplies, and disposition of assets to joint commanders, their forces, and the NCA within specified time frames.
- Ability to obtain and use combat and administrative support information from national, allied, coalition, and other widely dispersed assets.
- Collection, processing, storage, distribution, and display of information horizontally and vertically throughout organizational structures across the Battlespace.
- Rapid and seamless flow and exchange of information around the globe, enabling collaborative mission planning and execution from widely dispersed locations and at different levels (to include strategic, operational, tactical, and business).

The GIG provides a set of value-added functions operating in a global context to provide processing, storage, and transport of information; human-GIG interaction; network management; information

dissemination management; and information assurance. These functions are fully interrelated, integrated, and interoperable with one another in order to achieve overall interoperability across the GIG. As a result, the GIG is an information environment comprised of interoperable computing and communication components [4].

3.2 GIG Enterprise Services

The technical vision for the GIG is everything but DoD specific. The architects of the GIG vision used commercially supported and viable solutions to serve as a reference when blueprinting the future support for Command and Control. The best example is the concept of the GIG Enterprise Services (GES).

Enterprise Services is a term that refers to a high-level cross-entity Web Services-based component that satisfies the design goals of loose coupling, broad application, inherent security, availability and reliability, reduced cost and complexity, and increased levels of interoperability and information sharing. Enterprise Services provide 'organizational level' capabilities (i.e. system wide monitoring and security) that are typically utilized and leveraged by other Web Services (that may either be Enterprise Services or more low-level services) to develop specific functionality in all levels of the system. The ability to easily and efficiently integrate (utilizing SOAP or other technologies) with other services is a key differentiator between Web Services and past technologies. When properly designed and deployed, Enterprise Services can provide a dramatic increase in performance, capability, stability, and flexibility.

The leveraging "technology" here is a community based, open standard (Web/Enterprise Services) that has evolved based on mutual need and market forces. While there are other possible approaches (such as Government mandated software), utilizing a market based approach and leveraging widely available commercial services reduces cost and institutional resistance in adoption.

The critical role of GES in an integrated, Network Centric, Joint C4I (JC2) architecture can not be understated. JC2 will require new capabilities, and C4I architectures will require transformation from hierarchical, distributed, broadcast systems to systems designed to support NCOW.

As already noted, many of these Joint NCOW requirements have analogs in the marketplace, and the Enterprise Services approach allows us to adopt “best of breed” solutions and reduce development cost and risk. Another benefit is that commercial applications may be adapted more easily to joint military use as the system evolves, leveraging the investment and experience of others. Developing specific Communities of Interest (COI) for specific operational advocacies is essential. Each tailor able mission area should be represented by its own COI, in the requirements, development, testing, and fielding of mission applications to support that COI.

There are some obvious COI for the GES namely Services for the National Intelligence Domain (Title 50) and National Defense Domain (Title 10). The Defense Domain can be further subdivided into a Business Operations Domain and a Warfighter Operations Domain. The Business Domain could include COI for: Acquisition and Procurement, Installations and Environment, Human Resources, Logistics, Strategic Planning and Budgeting, Finance, Accounting, and Business Operations among others. In the Warfighter Domain, COI could include: Command and Control, Force Application, Force Protection, Force Logistics, Intelligence, and Battlespace Awareness. In addition to these “pure” COI, so called “cross COI domains” will be established as well, e.g., the Common Operational Picture COI supporting all Warfighter COI. M&S can be seen in a similar role.

3.3 Net-Centric Data Issues

One of the most radical changes is the data policy in the GIG. This is based on the DoD Data Strategy that postulates all data, regardless of the final consumer, will be available to selected users (theoretically anyone, anywhere with granted access) on “publish-subscribe,” “smart-push-pull,” or query-response type mechanisms. This is in sharp contrast to current data “stovepipes” that have been established by C4I system design or by doctrine that fails to make data available until after processing by the appropriate entity, often long after it is tactically useful by another community.

An example of this might be data collected for intelligence purposes that if shared before analysis processing might be useful to the Theater Commander for tactical uses, but if shared after processing is tactically no longer relevant (“If it isn’t timely, it isn’t tactical!”). In the DoD Data strategy, this sharing and posting of all data, will be ubiquitous in the GIG.

3.4 Security

Finally, it is important to add that the GIG will use “black” (i.e., not secured) transportation layers to send and receive “red” (i.e., classified) data as well as “black” data. This will be enabled by end-to-end information assurance and advanced cryptology. Security can be content based, and Public Key Infrastructure procedures can be applied.

The technical benefit is that the Internet Protocol (IP) can become the common basis for all shared solutions. GIG components can utilize the Internet or a DoD secure Intranet, special IP based hardware like the Joint Tactical Radio System (JTRS), the optical systems of the GIG – Bandwidth Expansion (BE), and more. This allows the application of standard, commercial distributed technologies, such as the already mentioned Web Services.

4 Joint Command and Control (JC2)

The transformation of the infrastructure is accompanied by the transformation of the processes. Command and Control will become more inter-service than it is today, leading to the processes underlying Joint Command and Control (JC2).

JC2 will consist of the trained personnel, policy, procedures, joint mission capability packages based on GIG infrastructure required to plan, execute, monitor, and assess joint and multinational operations. It is the logical follow on to the Joint GCCS vision and experience with the Defense Information Infrastructure Common Operating Environment (COE). The supporting JC2 architecture will enable the Joint Warfighter to accomplish assigned missions with greater speed and efficiency, improved interoperability, and reduced logistics support requirements.

The JC2 COP will present timely, fused, accurate, assured, and relevant information that can be tailored to meet the requirements of the Joint Force. Essential to the JC2 COP is the construct of a virtual warehouse of information – tracks, friendly and enemy force dispositions (aerospace, land, sea); intelligence, maps, and imagery; environment, logistics, and planning data; weather, socio-economic, and cultural information. Users will access the virtual warehouse to extract the set of timely, fused, assured, and relevant information they need to accomplish their mission. It is access to the COP combined with collaboration that will enable Commanders and staffs to achieve a high degree of shared Battlespace awareness.

Clearly, there is a need to tailor C4 systems to a particular use or interest area, much the way the Navy Component Warfare Commander concept decentralizes command and control in a time sensitive environment. In order to achieve the ability for a Commander to obtain timely situational awareness of the myriad of data available in a NCW environment, a “relevant” operation picture has to be presented to the Commander, with the ability to be selected from a “family” of possible configurations and options for a selected mission area. This picture must also be completely “integrated” for that mission area so that no information is omitted, but is also presented with due regard to information overload. Finally, there also must be the ability for C4I applications to “help” the commander utilize that information by either processing raw data for human cognition, or “sense-making” in a data overload situation. An example could be:

A “data mining” application to assist the Commander in finding and recognizing key intelligence data from available raw sensor data. This “sense-making” application could timely key the commander to perishable data that otherwise would be lost, or only available after lengthy analysis when no longer timely and tactically significant

5 Network Centric C4I Architectures

Currently, there is substantial effort in defining what is a Network Centric C4I architecture. The DoD Architecture Framework Version 1.0 (DODAF), is currently available, specifying common DoD architecture descriptions and data, as well as defining the relationships between various parts of the overall architecture.

The DoD Net-Centric Operations and Warfare (NCOW) Reference Model, has the goal of providing a common lexicon for NCOW concepts and terminology, supported by recognizable architectural descriptions. It is intended to be used as a model by systems architects for designing in Net Centricity as a fundamental part of the C4I system, vice an afterthought.

While improved ways of visualizing a Net Centric architecture (OV’s, SV’s, TV’s etc) are currently under development, the specificity in the architecture documents of Net Centricity required by the DODAF in every area ensure that the system backbone will be there to support NCOW applications in future C4I systems.

6 Examples of M&S Based Network Centric C4I Applications

The next generation of IT supporting JC2 must be much more agile than the C4ISR systems are today. The COP is still a quasi-static display of the situation, with latency issues, though promise is shown in the GCSS and I3 applications for the GCCS, a geospatial representation of logistics and intelligence data respectively. What the Warfighter needs is support in the agile JC2 process, i.e., tools that bridge the gap between the information domain and the cognitive domain. To make the COP vision of a “virtual warehouse” of data a reality, there is a clear requirement in the various components of a Network Centric C4I system to utilize Models and Simulations as part of applications. These can be the basis for planning and decision support tools, as well as the information processing required for visualization and presentation of information domains outside the normal COP physical geospatial domain. There are explicit and implicit requirements for sophisticated processing of that information and data for situational awareness, decision support, and operational control.

For example: a 3-D geospatial view of the radar electromagnetic space surrounding an afloat battle group, with platforms, sensors, terrain, and atmospheric conditions provided from the C4I system, would provide the commander valuable insight for force defense. A broader “Electromagnetic Operational Picture” could provide situational awareness of own force vulnerabilities (i.e., detection versus counter detection for various Emission Control conditions, jamming effectiveness, etc.) to support decisions in strike planning against enemy targets and protection from hostile force activities [7].

This example is an instantiation of one of many in the NCOW Information Domain, and we can see models and simulations will be at the core of these NCOW applications to provide this type of information to the Commander.

Previously the most promising approach to yielding these advanced applications has been the embedding of models and simulations into the COE [8]. As COE transitions to the GIG Enterprise Services these COE Embedded Simulation Infrastructure services will need to be part of that transition in order to meet the stated requirements of the GIG and JC2.

Key to making that transition is to ensure that GIG Enterprise Services have M&S integration, not just interoperability, as part of the overall requirements for these services. When reviewing the requirements for a

Network Centric system like JC2, or the Army Future Combat System, there clearly are implicit requirements for M&S as the enabling technology for new required capabilities. Similarly, when reviewing the GIG Enterprise Services requirements, these implicit requirements for M&S integration in the architecture are apparent.

With NCOW providing many paths for information to and from every node in the network the need for sophisticated underpinning Enterprise Services utilizing M&S is apparent. Clearly, the desired approach is to harmonize NCOW and Enterprise Services with the evolving M&S architectural concepts such as the XMSF.

7 Common Architectural Frameworks for the M&S and C4I Domains

A more SISO and simulation centric view of a common infrastructure was already proposed in [9]. This chapter draws a more broad picture of web-services and open standards applicable to both domains of interest in this paper, future M&S and future JC2.

7.1 The Extensible Modeling & Simulation Framework (XMSF)

XMSF is intended to contribute to the transformation of the armed forces by contributing to fulfill the requirements for software system support derived from future military operations. Concerning the XMSF group, the only software systems that composably scale to worldwide scope utilize Internet and web technologies. The XMSF Reports available on the XMSF website¹ present the consensus integration of extensive inputs by over 50 experts participating in several workshops. By embracing commercial web technologies as a shared-communications platform and a ubiquitous-delivery framework, DoD M&S can fully leverage mainstream practices for enterprise-wide software development. The use of open web-based standards and technologies doesn't imply that XMSF is limited to the public Internet. The actual Working Definition for XMSF is:

“The Extensible Modeling and Simulation Framework (XMSF) is defined as a set of web-based technologies and services, applied within an extensible framework, that enables a new generation of modeling & simulation (M&S) applications to emerge, develop and

¹ Everything produced under the aegis of XMSF, including position papers of experts, links to other institutions, etc., can be found at <http://www.movesinstitute.org/xsmf>.

interoperate.

Current work in Web Services appears to be an appropriate basis for organizing and composing the many necessary capabilities of Web/XML and Internet/networking needed for M&S applications.”

XML-based markup languages, Internet technologies, and Web Services will enable a new generation of distributed M&S applications to emerge, develop, and interoperate.

Web-based technologies applied within an extensible execution framework are enabling a new generation of modeling and simulation applications to emerge, develop, and interoperate in the commercial world. A bridge is needed between these emerging commercial technologies/standards and defense systems. An extensible XML-based framework can provide a bridge between forthcoming modeling and simulation requirements and open/commercial Web standards.

7.2 Using Web Services for M&S

Why else are Web Services of interest in the context of Modeling and Simulation integration with Network-Centric Command and Control Architectures? The reason is that the fundamental idea behind Web Services is the integration of applications as services. The concept represents a defined set of industry-standard technologies that work together to facilitate interoperability between heterogeneous systems, whether within an organization or across the Internet. In other words, with Web Services we can web-enable applications to communicate with other applications that have been similarly enabled according to Web Services standards. This seems to be a tremendous opportunity to build bridges between former stove-piped developed systems. The idea itself is not new. At its core, Web Services are nothing else but another approach of distributed computing. However, looking at the commercial support of these concepts, it is definitely a viable one.

What are Web Services? Web Services can be defined as discrete Web-based applications that interact dynamically with other Web Services. In order to make this happen, several sub-functions are necessary, namely:

- Functionality self-description of the service
- Publishing of service descriptions using a standardized description
- Locating the service with the required functionality

- Requesting the required data to initiate the service
- Establishing the necessary data exchange with other Web Services, including delivering the results

The Web Services vision is that they will work together seamlessly because they are developed to the same standards for self-description, publishing, location, invocation, communication, and data exchange capabilities. All these standards are open standards, such as the web service description language (WSDL), the extensible markup language (XML), or the simple object access protocol (SOAP). Furthermore, these technologies chosen for Web Services are inherently neutral to compatibility issues that exist between programming languages and operating platforms. As a result, applications using Web Services can dynamically locate and transparently use necessary functionality, whether available locally or from across the Internet, regardless of the programming languages or operating platforms involved.

However, it should also be taken into account that, as Web Services proliferate, concerns including the overall demands on network bandwidth, and for any particular service, the effect on performance as demands for that service rise. A number of new products have emerged that enable software developers to create or modify existing applications that can be "published" - made known and potentially accessible - as Web Services.

What are implications for Modeling and Simulation integration with Network Centric Command and Control Architectures? It is perceived more than likely that Network Centric Command and Control Architectures will be based on the Global Information Grid (GIG) as defined in [5]. First administrative processes, such as a Network Centric Data Strategy as defined by the DoD CIO [11] and an overarching Data Management [12] have been established; however, the integration of M&S into these activities is only at its beginning. In order to achieve a common infrastructure as envisioned in earlier papers, a full integration of standardization efforts is necessary.

The first step is the integration of the M&S Name Space Management into the GIG Name Space Management. The next step is the definition of respective profiles; such as is initiated now in the Extensible Modeling and Simulation Framework (XMSF) Profile Study Group of the SISO. Furthermore, M&S application specifics have to be identified and captured in standards like web service

description languages. For challenges to be met in this context refer to [13].

In case of interest, a Study Group defining the constraints and requirements for M&S applications and components to become Web Services in general, and in particular to become Web Services within the GIG, could be very valuable.

The merging of the JC2 Web Service paths and M&S Web Service paths, such as XMSF, are valuable for both communities, as many services are needed in both communities. One of the best examples may be the domain of visualization, such as terrain servers and icon servers for symbols as defined in the military standard 2525. Common data servers based on a common ontology are another example. Some of these examples are currently under prototypical development by XMSF partners.

7.3 M&S Services in the GIG

The long-term goal to support the ideas proposed in this paper is the full integration of M&S services into the GIG. Three main application domains and related communities of interest (COI) have been identified so far:

- Establishing of M&S kernel services to enable advanced distributed simulation within the GIG and GIG Enterprise Services (GES). The RTI services can be seen as the hub for these M&S services, which have to be extended gradually. This approach is already described in [10] for the general case.
- Establishing a Training Community of Interest, e.g. in conjunction with the establishment of the Joint National Training Capability (JNTC) in addition to the already defined COIs for Command and Control, Force Application, Force Protection, Battlefield Awareness, and Logistics.
- Establishing M&S Support as a Cross-Domain COI, similar to the actual Common Operational Picture (COP) Initiative, being of importance to all COI of the Armed Forces.

These ideas are far from being mature. They should encourage the beginning of a discussion between simulation developers, simulation users, and standard developers.

To this end, SISO already is contributing to specific symposia organized under the aegis of the Object Management Group (OMG), the Open GIS Consortium

(OGC), the Web 3D Consortium (W3C), and SISO.² In the mid term, these combined efforts must lead to the establishment of standards within SISO and the broader enterprise driven context.

Another aspect of importance is the data and information obtainability in the GIG. As noted before, data and information will be available within the GIG “within an instant.” If this data source can be made available to a M&S system, this would facilitate the data problem dramatically, and costs for exercises and events could be reduced drastically. The requirement, however, requires enforcement to support open standards for data import and export for legacy and future systems. The time of proprietary file structures and data models should be over, a well documented interface, using standards such as the XML, should be the rule for every system of operational interest, which implies publishing of the related information and the coordination of the terminology in the M&S namespace.

7.4 The next Order-of-Magnitude Improvement for Command and Control

The Network Centric Operations and Warfare (NCOW) value chain approach [3] employs several layered concepts:

- The value chain starts with *Data Quality* describing the information within the underlying command and control systems.
- *Information Quality* tracks the completeness, correctness, currency, consistency, and precision of the data items and information statements available.
- *Knowledge Quality* deals with procedural knowledge and information embedded in the command and control system such as templates for adversary forces, assumptions about entities such as ranges and weapons, and doctrinal assumptions, often coded as rules. In future systems, this agile component could be presented by M&S systems. Knowledge quality is the first component related to the common model of the operation.
- Finally, *Awareness Quality* measure the degree of using the information and knowledge embedded within the command and control system. Awareness is explicitly placed in the cognitive

domain, i.e., definitely above the level of technical interoperability.

In summary, the ability to share data, information, knowledge, and awareness enables conducting operations more efficiently.

The authors are proposing the view, that the NCOW value chain is companioned by the IT value chain reflecting C4ISR improvements over the recent decades. C4ISR systems started as database centric and message driven solutions. They were only able to support Data Quality. To support the next level within the value chain, the idea of the Common Operational Picture (COP) had to be introduced. This led to a jump in the quality, i.e., increasing it by an order of magnitude (a picture says more than 1,000 words). The reason is that the COP added context to the data, hence increased not only the Data Quality, but also Information Quality. The introduction of M&S to C4ISR adds procedural knowledge in form of models; hence, the next level in the value chain can be supported, which will lead to another improvement (a simulation says more than 1,000 pictures).

The integration of M&S components into the IT infrastructure therefore is seen as an operational necessity. The technical requirements are given. Similar to NCOW, it is more the need to bridge the cultural gaps than the technical gaps to make this vision become reality.

8 Summary

The command and control community is shifting from the system centric view to the network centric view. While until recently this was mainly limited to the conceptual preparation of the transformation of the armed forces, the advent of the Global Information Grid (GIG) and the GIG Enterprise Services (GES) is now enabling the technical implementation of the underlying ideas. Network Centric Operations and Warfare (NCOW) as envisioned by Alberts et al. [3] is finally becoming a reality. Joint Command and Control (JC2) is on its eve of implementation. Operational M&S functionality is technically ready to be integrated and operationally required to support modern military operations. NCOW has hard requirements for this M&S functionality. The necessary standardization effort to harmonize M&S standards with the GIG requirements, and even more important, the transfer of advanced M&S requirements of operational importance to the GIG [13], must become a future topic within SISO and the broader military COI.

² For details on the Web Enabled Modeling and Simulation Network, please refer to the website <http://www.websim.net>.

9 References

- [1] Carl von Clausewitz: "On War", translation by Colonel J.J. Graham published by N. Trübner, London, 1873.
- [2] Report to Congress: "Network Centric Warfare," The Pentagon, Washington, D.C., July 2001
- [3] David S. Alberts, John J. Garstka, Richard E. Hayes, David A. Signori: "Understanding Information Age Warfare," CCRP Publication Service, August 2001
- [4] U.S. Department of Defense: "GIG Capstone Requirements Document," August 2001
- [5] U.S. Department of Defense Directive (DODD) 8100.1: "Global Information Grid (GIG) Overarching Policy," The Pentagon, Washington, D.C., September 2002
- [6] U.S. Department of Defense: DoD Data Strategy
- [7] Daly, J, Layman, G.: "C4I Tactical Applications Utilizing Embedded Simulations" Command and Control Research and Technology Symposium (CCRTS), June 11-13, 2002; Naval Post Graduate School, Monterey, California.
- [8] Layman, G, Daly, J "Integrating Simulations into DII COE Compliant C4I Systems" 02F-SIW-048, Fall Simulation Interoperability Workshop, Orlando, Florida, September 2002
- [9] Andreas Tolk: "A Common Framework for Military M&S and C4I Systems," 03S-SIW-031, Spring Simulation Interoperability Workshop, Orlando, Florida, April 2003
- [10] Andreas Tolk: "Avoiding Another Green Elephant – A Proposal for the Next Generation HLA based on the Model Driven Architecture", 02F-SIW-004, Fall Simulation Interoperability Workshop, Orlando, Florida, September 2002
- [11] U.S. Department of Defense, Chief of Information Operations (CIO): "Department of Defense Net-Centric Data Strategy," The Pentagon, Washington, D.C., May 9, 2003
- [12] U.S. DoD Data Management; Congressionally Directed Action, House of Representatives Report 107-532 DoD, 15. March 2003
- [13] Andreas Tolk: "The Levels of Conceptual Interoperability Model," 03F-SIW-007, Fall Simulation Interoperability Workshop, Orlando, Florida, September 2003

10 Authors' Biography

JOHN J. DALY is a Research Engineer with Booz Allen Hamilton working in the Architecture Analysis area for the Department of Defense. John previously worked with the Naval Research Laboratory, in Command and Control system development with responsibilities in: C4ISR/Simulation Interoperability, the Embedded Simulation Infrastructure, and GCCS Embedded Training Technologies for C4ISR. A retired Naval Officer, John served on the staff of the Director, Defense Information Systems Agency, as well as in the DISA Modeling and Simulation Directorate working on C4I and simulation interoperability.

ANDREAS TOLK is Senior Research Scientist at the Virginia Modeling Analysis and Simulation Center (VMASC) of the Old Dominion University (ODU) of Norfolk, Virginia. He has over 12 years of international experience in the field of Applied Military Operations Research and Modeling and Simulation of and for Command and Control Systems. In addition to his research work, he gives lectures in the Modeling and Simulation program of ODU.