

**11th International Command and Control Research and
Technology Symposium
“Coalition Command and Control in the Networked Era”**

Fortis Adnexus (NexNet)

“Concept Exploration into Future Planetary Command and Control”

Topics: C2 Concepts and Organizations
C2 Architecture
Coalition Interoperability

Mr. Samuel R. Oppelaar Jr.
L-3 Communications-Titan Group, Incorporated
7104 Laird Street
Panama City Beach, FL 32408

(850) 230-7283 (Office)
(719) 930-8487 (Cell)

samuel.oppelaar.ctr@navy.mil



FORTIS ADNEXUS: Strong, Powerful, and Robust Connection
“NexNet”

Abstract

This paper is the third in a series¹ of concept exploration papers that together describe future concepts in Command and Control (C2) in the Networked Era. While great advances have been made over the past few years in C2 concepts and architectures, we are still in search of a real solution to enabling C2 across militaries, nations, supporting government and non-government agencies, and coalitions. The previous paper introduced the concept of “Poly-Discipline Command”² as a conceptual framework for integrating the instruments of national (and coalition) power into a seamless organizational entity. This paper explores the concepts associated with the development and capabilities needed to enable that concept, and then execute C2 across national, political, and military force structures, and to effect coherent and coordinated operations anywhere on the planet. While there has been extensive effort to standardize interface and interoperability requirements for access to and use of the Global Information Grid (GIG), there has yet to emerge a singular conceptual “network” or “system” that is structured to truly integrate C2, planning, operations, and execution in the “Poly-Genetic”³ arena of future operations. Specifically, this paper explores a conceptual C2 environment (Fortis Adnexus) called “NexNet”.



¹ Refers to SYNAPSE: Poly-Genetic Quantum Architecture for Command, Control, and Execution, and Poly-Discipline Command and Transactional Command Authorities

² Oppelaar, Samuel R., Jr., Poly-Discipline Command and Transactional Command Authorities, 10th ICCRTS, June 2004.

³ Description of a system’s origin that is beyond “conceived joint”, to one that is conceived to incorporate military, political, non-government agencies, international organizations, and coalition elements.

Introduction

We live in a world today whose security climate dynamically changes as rapidly as new threats emerge from terrorist organizations, rogue nation-states, and fundamentalist regimes. These threats to our security at home and abroad have shifted significantly from traditional forms of conflict that employ national armed forces against each other, to extremely complex efforts to neutralize non-traditional threats to security. In the aftermath of Operation Iraqi Freedom, the entanglement of nation reconstruction with insurgent terrorism presents a symptomatic snapshot of the security challenges we are likely to face many times again. It is this environment that has prompted the military establishment to refocus the priorities of defense acquisition away from the mass of firepower, and toward enhancement of intelligence gathering and processing through network and information warfare. This security environmental shift was recently conveyed to leadership of the defense industry in comments made by Principal Deputy Under Secretary of Defense for Policy, Mr. Ryan Henry.⁴

Mr. Henry told the contractors that the Pentagon was redefining the strategic threats facing the United States. No longer are rival nations the primary threat - a type of warfare that calls for naval destroyers and fighter jets. Today the country is facing international networks of terrorists, and the weapons needed are often more technologically advanced, flexible and innovative.

In addition to this security challenge backplane, national, international, and non-government organizations have been challenged to respond to natural disasters and relief operations in the past year that stagger our imagination to understand their human impact. The relief operations that resulted from the Tsunami of 26 Dec 04, multiple hurricanes devastating areas of the United States in 2005, and the earthquakes that caused countless loss of life in Pakistan this year, demanded huge responses on a planetary scale.

Command and Control (C2) as many of us conceive it, refers to C2 of military forces engaged in some type of activity, be it force application, peacekeeping, or conducting humanitarian relief operations. We need to begin understanding and conceiving C2 on a much broader scale if we expect to succeed in securing peace and providing coordinated responses to other forms of disasters that occur on the planet. This coordinated application of national and international power is described in the concept of "Poly-Genetic Organizations", where assembling the instruments of national power to respond to planetary

⁴ Leslie Wayne, *Contractors are Warned: Cuts Coming for Weapons*, New York Times, 27 December 2005

events (either security or otherwise) involves a complex fabric of interrelated sources, not just military. Within the military construct we recognize the concepts of a Joint Force, a Combined Coalition Force, or Alliances, each with their own C2 “systems”. Over the past decade, we have seen the emergence of euphemisms such as “interoperable”, “born joint”, and even “conceived joint”. These terms describe how we approach acquisition, design, and fielding of systems that support military operations. The continuing effort to conceive joint systems has been a good one, resulting in systems that are able to “talk to each other”, communicate, share databases, all while displaying the veritable common operational picture (COP), and most recently the user-defined operational picture (UDOP).

As a follow on effort to the recent DoD Quadrennial Defense Review (QDR), Deputy Defense Secretary Gordon England is directing the formation of eight new “QDR Execution Roadmaps”. Of the eight, two in particular could have significant impact on our conceptual thinking of command and control. Descriptions of these efforts are extracted below.⁵

- “Authorities,” led by Pete Geren, special assistant to the defense secretary, and Army Lt. Gen. Raymond Odierno, assistant to the chairman of the Joint Chiefs of Staff. This body will suggest legislative and regulatory changes to ensure “operational effectiveness in the face of new threats.”
- “Joint Command and Control,” led by John Grimes, assistant secretary of defense for network and information integration, and Army Lt. Gen. John Wood, deputy commander of U.S. Joint Forces Command. This effort will examine issues related to fielding, management and governance of command and control capabilities.

In the sections that follow I will introduce a new concept in C2 delivery. It is based on the premise that “operations”⁶ conducted in the future, whether to engage an asymmetric threat from the entities discussed above, or other types of planetary actions where a coordinated delivery of services and force may be necessary, inclusive of non-military entities, will demand a C2 environment (or system) that enables all agencies to operate on a common platform, use common collaboration protocols, while providing strong, powerful and robust connectivity...**Fortis Adnexus**, or **“NexNet”**.

⁵ Sherman, Jason, *England Orders Eight QDR Spin-Off Reviews*, Inside Defense, 10 January 2006.

⁶ In this context, “operations” refers to the application of instruments of national and international power that includes actions and activities that are not strictly military, but include those of other agencies, power centers, organizations, and their influences on a continuum of actions that may or may not include combat force to accomplish national objectives within a crisis or conflict area of the planet.

We will begin the exploration of NexNet with a short review of the “Poly-Genetic” concept of systems and application of power. This in turn leads to a more in depth look at the NexNet conceptual environment. And finally, we will explore in some detail the NexNet conceptual system, its construct, basic capabilities, and utility to meet the security challenges of the 21st Century.

Poly-Genetic Operations

Nearly every operation undertaken by the United States in recent memory, whether military force-centric or otherwise, involved the participation of many federal government agencies and departments, in some cases state and local governments⁷, and broad participation of the United Nations, NATO, and Allied Governments dealing with international events. This is the very nature of operations globally as a result of the evermore-complex fabric of international power and society. Speed of communications, transportation, and information sharing on a planetary scale has resulted in an interdependent relationship amongst the nations and peoples of the planet. This interdependence now demands increasing closer working relationships, international cooperation, and sharing of information, resources, and capabilities to achieve national and international objectives for peace and prosperity.

The concept of Poly-Genetic operations in some respects describes what we have already been doing when mounting an operation...applying sanctions, exerting diplomatic pressures, leveraging political processes, and the threat of force if necessary. But historically, nations have employed these instruments of national power in a linear fashion, one after another until something works. Within the Poly-Genetic construct of operations, instruments of national power are integrated in advance of “situations” or crises, planning together as a team, then executing as a team. The team may be a combination of national assets, or one that is international in scope and character (including non-government organizations). Even with the US Joint Forces Command deployment of the prototype Deployable Joint Command and Control System and the excellent service-centric voice and data services it provided, integrating military and civil agencies into a singular collaborative C2 environment was problematic at best.⁸ And the US Congressional Report on Katrina Response has this to say about the overall coordination effort:⁹

The Homeland Security operations center failed to provide important situational information to the White House and other key officials during the disaster.

⁷ Katrina Relief: FEMA, US Coast Guard, Military Forces, States of Louisiana and Mississippi Emergency Response Teams, and City of New Orleans.

⁸ Extracted from Joint Task Force Katrina (JTF-K) Joint Force Maritime Component Commander (JFMCC) Command and Control, Communications, and Computer (C4) Lessons Learned (Draft), 25 Sep 05. (Unclassified)

⁹ Special House panel's findings on the government's response to Hurricane Katrina and in the days immediately after the Aug. 29 storm, The Tucson Citizen, 13 February 2006.

The overall goal then of the NexNet concept is to establish a C2 environment that can dynamically link using a common toolset and application framework, the entire Poly-Genetic community that consists of national, non-government, and coalition power centers. This is also one of the stated goals for net-centricity in the 2006 Quadrennial Defense Review.¹⁰

Develop an information-sharing strategy to guide operations with Federal, state, local and coalition partners.

QDR Extract, 6 Feb 2006

Homeland Security Adviser, Frances Fragos Townsend, as reported by the Baltimore Sun, recently sounded the call for a system that reflects NexNet's capabilities.¹¹

"We need a national [communications] system that ensures operability, survivability and interoperability..."

The Conceptual C2 Environment of Tomorrow

Over the past decade we have seen a dramatic transition of our security threats, along with planetary and natural events that have demanded coordinated responses by government, non-government, and international agencies. The threat transition away from a "force-on-force" paradigm toward combating the asymmetric threats of terrorists, Islamic Fundamentalist militant groups, and loosely confederated insurgencies collectively require that virtually all interested sources of power, both domestic and international, be called into action to support operations. As described in a previous paper on C2, "operations" can no longer simply mean "military", but now should be considered as the coherent application of multiple sources of national power. In today's "operations", whether led by a military command structure, or civilian authority, extensive real-time and effective collaboration is essential for success. One only has to recall the confusion and lack of coordination extant during the aftermath of Hurricane Katrina to understand the principle here.

As we move ahead into the unknown of future calamity, we should have the capability and understanding to conduct operations across governments, non-government agencies, and coalitions. This new capability must transcend existing communications systems and provide a network-centric solution to conducting operations on a broad collaborative scale. In tomorrow's C2 environment, all sources of power (and support) will have the capability to access

¹⁰ United States Department of Defense, Quadrennial Defense Review Report, 6 Feb 06.

¹¹ Bowman, Tom, "Lessons Learned" Review, Baltimore Sun, 23 Feb 06.

a planetary C2 network and tool set capable of planning for operations on a broad scale, integrating efforts of participating agencies and forces, the then executing operations with precision, shared understanding, and force-multiplied effectiveness. Advancements in information technology and communications systems provide us with the basic tools to establish command and control of the poly-genetic operations of the future, but haven't yet responded to the requirement for a fully dynamic and flexible C2 environment that transcends agency boundaries. Virtually all government departments and agencies have their own network and information systems to support their specific missions. These systems house extensive information databases and capabilities needed to perform their missions, but rarely provide shared access to data and existing legacy C2 systems, and do not allow for cross-boundary collaboration capability except perhaps for email. For example, even within the US Department of Defense (DoD), there isn't a universal collaborative tool in use. The DoD's standard is the Defense Collaborative Tool Suite (DCTS) managed by the Defense Information Systems Agency (DISA), but other tools such as InfoWorkStation (IWS), and "Groove Virtual Office" are employed by various services and combatant command components. During Operation IRAQI FREEDOM for example, the USCENTAF Combined Aerospace Operations Center (CAOC) was using IWS, while other DoD entities used DCTS. In fact, the new Deployable Joint Command and Control (DJC2) system in present production has both IWS and DCTS services organic to the system as part of its Collaborative Information Environment (CIE).

Now we need a C2 environment that goes beyond "conceived joint" along the spectrum of operability to one that is "poly-genetic" in its design, employment, and mandate. The mandate must be generated at the highest levels of government, who should now say, "Give me a way to coordinate all the instruments of national, international, non-government, and coalition power in a single planetary command system." "I want everyone to be able to collaborate on planning so we can reduce or eliminate confusion when we have to apply resources and forces." In the complex security and operational challenges that we'll face in the future, we must be able to overcome the C2 disconnects that have plagued us in the recent past.

NexNet Concept and Design

The NexNet concept of Command and Control represents a disruptive innovation in both thought and function. In order to grasp this concept, we must envision a capability that does not yet exist. To begin with, NexNet is not just a machine, nor is it a network identified in present understanding. In this new conceptual world, NexNet provides a capability to for all government, military, and international coalition elements to actively interact with each other, to plan together, get direction, collaborate, and to execute operations in a synergistic application of power. In concept, NexNet has the ability to link participants through web-centric access to a core environment that links legacy command

and control systems, shares data bases, and provides a centrally managed collaboration capability. This aspect of NexNet shares the concept of a “Service-Oriented Architecture” (SOA), where service consumers (the users) access applications and services provided by service providers that are “exposed” to an interface allowing the consumers to directly access the particular service. The following description explains the SOA concept further.¹²

In the emerging net-centric environment, as organizations strive for greater flexibility and interconnectivity there is a movement from organizing around systems, to organizing around services. In a *Service Oriented* world, the capabilities and data encapsulated within a system are broken apart and exposed via the network to third party customers. This has great benefits for customers, as they can dynamically discover and utilize the capabilities and information they require without the need to acquire, operate, and maintain a specialized system for doing so. It also has great benefits for service providers, as the cost of entry and time for providing services can be significantly reduced without the need to deliver them as part of a complete system.

In conceptual theory, the NexNet system will provide a single network gateway for all participants to log into. The gateway performs a number of functions to include managing the security level of access for the participant. The gateway will run in a multi-level security protocol. It will be able to determine what level of access each participant will receive based on the participant’s login credentials and the system being used to access the NexNet. For example, if a person logs onto NexNet using a cleared classified system at the “Secret” level, and has cleared credentials for this level, the NexNet will grant access to information, databases, and applications at this level. Also, if a participant is logging in at the “Unclassified” level from any unclassified network system, then NexNet will allow access only to unclassified data, collaborative tools, email, data bases and applications. Some “situation awareness” applications, such as the “operational picture”, may be available at the unclassified level depending on the type of operation. The gateway is the single point of entry into the NexNet, and provides all users with a redundant and powerful set of applications that can enable military forces (both domestic and coalition), local, state, and federal government agencies, and non-government agencies such as the Red Cross, to access a common collaboration environment where they can plan, communicate, and execute complex “operations”. NexNet access will be centrally controlled and managed by the NexNet gateway. Individuals and organizations are provided with a NexNet-unique user name, password and biometrics called the NexNet Access Set (NAS). The NexNet uses the NAS as a basis for collaboration, information sharing, application access, and command and control processes. Figure-A below illustrates the “Operational View” of the NexNet Concept.

¹² Allen, Bernal B., A Strategy for Managing the Development and Certification of Net-Centric Services within the Global Information Grid, Defense Information Systems Agency (DISA), 27 September 2005.



Figure-A
NexNet Operational View

NexNet Environment Structure

The NexNet environment includes the NexNet Tri-Core main processors, people (the users) and procedures. Each of these components relies on the other two to make the NexNet function.

NexNet Tri-Core Processor Set

The NexNet Tri-Core Processor Set provides the backbone of the connectivity and application processing and allows users to "log-in" to the NexNet C2 Environment. Each leg of the Tri-Core is identical while maintaining constant interface with the other two core components. One core is the active component, a second core operates in "hot parallel" and automatically assumes the active role without service interruption, and the third core rests in warm standby, while maintaining database images and applications mapping. This Tri-Core arrangement provides unprecedented computational power and fail over

protection. The components of the Tri-Core would be geographically separated to further enhance passive defense against kinetic attack. The NexNet C2 Environment operates in a simultaneous multi-layer security field, where access to applications, data, communications, and displays is commensurate with the security level of the user.

Users

The very nature of a command and control system involves people. The implication is that for NexNet to function, the right people (or agencies) need to be logged into the system and operating. Within the concept of "Poly-Genetic" operations, it is essential that standing units and agencies plan together in advance of any potential crisis or emergency to effect a smooth transition from a state of equilibrium¹³ to a state of a self-organized open system that results from applying energy across the system in the form of operational inputs. In a crisis situation, energy is injected into the system through information, intelligence, commands, instructions, and collaborative planning. The desired result of this application of energy into the system is the self-organizing power of all of its participants into a very ordered state¹⁴. Translated, this means that the confluence of the inputs made by participants (leaders, commanders, units, agencies) results in coordinated planning, action, and execution.

Procedures

As described earlier in this paper, the NexNet conceptual environment would bring together a vast conglomerate of people and organizations that may be engaged in an operation. For this large contingent to work effectively together there is a need for clearly understood procedures for operating within NexNet. As NexNet matures from this concept stage through its development life-cycle, the users (warfighters, national governments, international organizations, and non-government agencies) will participate in NexNet development and socialize the concept in advance of deployment. Users will be directed at the highest levels to employ the NexNet if they wish to participate (or are directed) in any given crisis or operation. Protocols established by the NexNet controlling authority will guide users from all disciplines on how to best integrate and participate in operations being planned, coordinated, and executed via the NexNet.

¹³ Atkinson, Simon Ray, and Moffat, James, The Agile Organization, Command and Control Research Program, July 2005, pg 24.

¹⁴ Atkinson, pg 32.

NexNet Functional Capabilities and Applications

In this section we'll look at the unique capabilities that makes the NexNet environment such a power tool for command and control on a planetary scale. The capabilities are grouped by functional area. **Figure B** below illustrates the functional capabilities of NexNet.

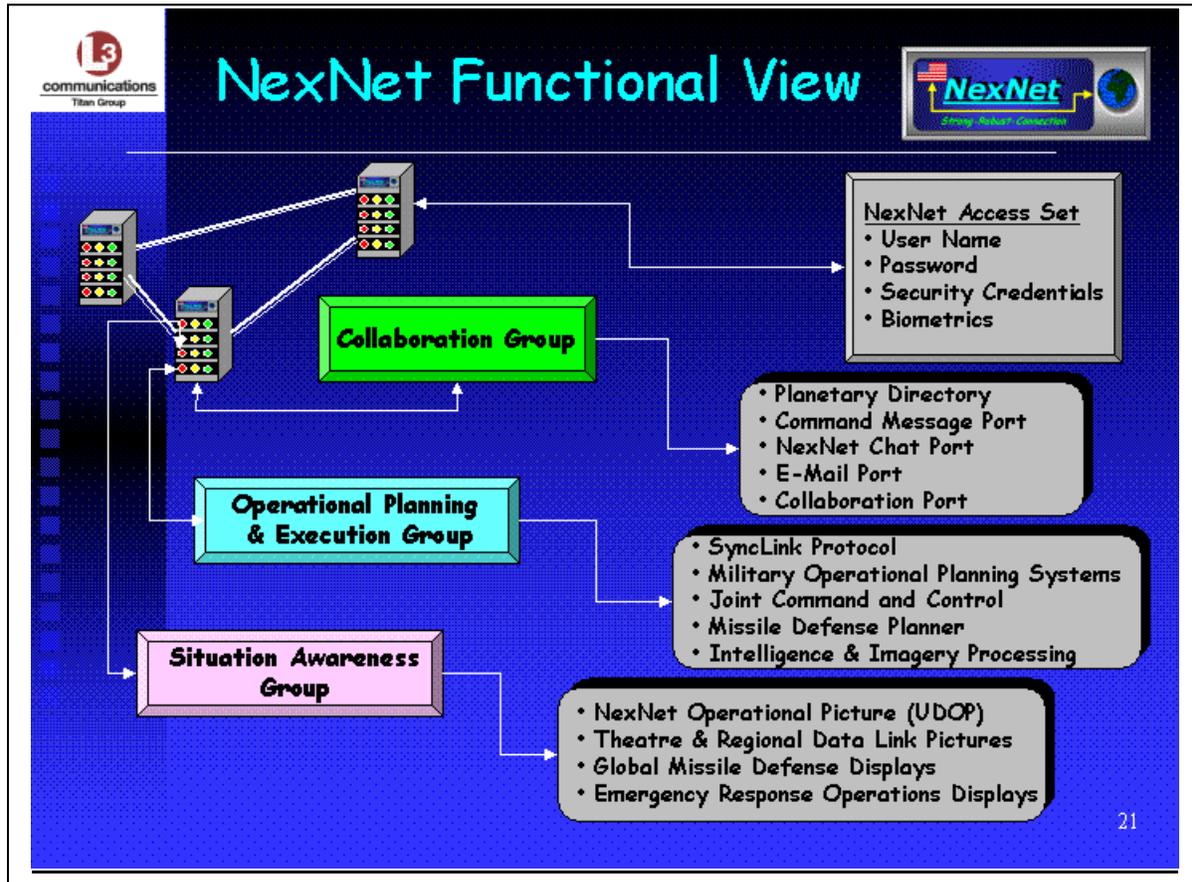


Figure B
NexNet Functional View

Collaboration Group

This group may represent the single most important capability that continues to elude the joint and coalition military community, but more importantly, the capability for military forces to effectively collaborate with civilian counterparts. The NexNet solves this problem by providing a set of common¹⁵ collaboration tools that all users will use to communicate with each other, either at the organization or individual level. These tools run on the main NexNet

¹⁵ "Common" in this context means that every user of the NexNet, has access to the same collaborative tools that are linked by the NexNet via its multi-level security protocols, allowing direct synchronous and asynchronous collaboration, information exchange, and application visibility for all participants.

system, independent of service, organizational, and national systems. The NexNet collaboration group provides the real link between deployed military forces, national, state, and local governments and agencies, and non-government entities that may be supporting a particular operation. Now let's look at the components of the *Collaboration Group*.

Planetary Directory: The planetary directory within NexNet is the foundation of participants NexNet uses to facilitate all collaboration tools within the group. The planetary directory is accessible by all users. The *Planetary Directory* is accessible from any of the *Collaboration Group* components.

Command Message Port: This port provides commanders (or civilian leaders) at all levels with the capability to transmit command instructions to all members of a task force or operational grouping of participants involved in an operation. The originating official can select groups, units, agencies, and individuals to receive the command message. The messages will be instantaneous relayed to all selected recipients, who receive an alert on their NexNet screen that a command message has been received. When accessed, the message will include a date-time group (DTG) and identify the sender, classification, and priority.

NexNet Chat Port: The NexNet *Chat Port* is used to collaborate with any selected group, unit, agency, or individual who is active on NexNet.

E-Mail Port: All users of NexNet are provided with a NexNet email address that allows the user to send and receive normal email traffic to and from any global email address, both internal and external to NexNet.

Collaboration Port: The NexNet *Collaboration Port* operates like the *Chat Port* and includes access to file sharing¹⁶, white board, or situation awareness displays. The collaboration port also allows for Voice/Video over Internet Protocol (V/VoIP) capability. By selecting this feature on the *Collaboration Port*, the initiator is linked either by voice alone or both voice and video to the other selected users.

Operational Planning & Execution Group

This group of capabilities provides access to current (legacy) and future command and control planning and execution applications used by the military services and combatant commands. By accessing these applications via NexNet, no additional login credentials or steps are needed to access the applications. For example, if a NexNet user requires access to the Theater Battle Management Core System (TBMCS), by selecting TBMCS from the available applications, NexNet enters the TBMCS environment for the selected geographic region (SOUTHCOM, CENTCOM, etc), as a certified participant. NexNet performs this type of join through its "SyncLink" protocol.

¹⁶ Typical files may include word documents, power point presentation, imagery files, or other graphics.

SyncLink: The *SyncLink* protocol within NexNet enables direct access to the selected capability. NexNet connects to the target system by providing the user's NexNet Access Set (NAS). The capabilities available to the user based on their NAS are highlighted on the list of available *SyncLink* systems. All users will be able to "sync" with other agencies' databases and applications based on their NAS credentials provided by NexNet. For example, unclassified users may be able to access other unclassified information and data bases from participating agencies, government, non-government, coalitions etc. The list below illustrates some examples of capabilities accessible via NexNet's *SyncLink*:

- Theater Battle Management Core System (TBMCS)
- Space Battle Management Core System (SBMCS)
- Joint Operational Planning & Execution System (JOPES)
- Command and Control Battle Management & Communications (C2BMC) for Ballistic Missile Defense
- Global Command and Control System-Joint (GCCS-J) or the follow-on Network Enabled Command System (In early development as of this writing)
- Intelligence and Imagery Processing Applications

Situational Awareness Group

NexNet provides a menu of operational and battlespace situational awareness tools to the NexNet users. NexNet uses its *SyncLink* protocol to "connect" the user to the appropriate or desired display, as well as providing a generic unclassified display for general use. Users may select the display type from the available options in the *Situational Awareness Group*.

- NexNet User-Defined Operational Picture (UDOP): This is a planetary-wide display that can be defined by the operator to view specific selectable categories of real-time or near real-time data.
- Theater or Regional joint or combined data link displays to include air, space, surface, maritime, and sub-surface categories of tracking data. The user selects the theater of operations to "view" and NexNet provides a DoD standard background maps and overlays along with the selected category of data. Thus a user logged on in the CONUS can quickly view a tactical data link picture being produced by sensors and C4 systems anywhere in the world where US/Coalition forces are producing a data link operational picture. In both data link and UDOP displays, the user defines the type and category of information to be displayed. This may include geographic backgrounds and overlays, friendly and hostile forces and tracks, and other categories of order of battle symbology.
- Global Missile Defense Display: NexNet draws on data from national missile defense and early warning systems to provide the user with a near real-time display of potential or extant hostile missile launch events and defensive actions.

- Emergency Response Operations Display: This display is created by the command user specifically in response to a natural or other disaster that calls for a unified government, international, and non-government agency response. It can include area maps, transit routes, recovery centers, transportation and supply hubs/centers, and emergency response force symbology for participating forces and agencies.

Command and Control Above the Military Level

Throughout the description of the NexNet concept, we have alluded to the idea that Command and Control of “Operations” goes far beyond the military component. The nature of planetary operations today, some that involve political upheaval such as we are currently witnessing in the Middle East, terrorist and insurgency activity meant to disrupt peaceful coexistence in vulnerable areas, and international and domestic response to natural disasters on the scale of Hurricane Katrina or the Pakistan earthquake, involve executing command and control of disparate organizations and forces on a scale of immense proportions. The extract below by Dr. Alberts and Dr. Hayes from *Campaigns of Experimentation* describes the character of the prospect of “command and control above the military level”.

“Homeland Defense (a DoD responsibility) and Homeland Security (which DoD supports) have emerged as major challenges. These are inherently not only interagency (DoD, HLS, state/local government), but international and inter-sector (private, public) problems. While cabinet-level agreements exist on how they work from a federal perspective, the serious involvement of state and local authorities, as well as a host of private organizations (e.g., telecommunications companies, utilities, private hospitals, the Red Cross) and foreign governments most likely to be involved (e.g., Canada and Mexico) is also required for success. Even at the federal level, considerable potential exists for confusion becomes exacerbated.¹⁷

What this means is that Command and Control in the Network-Centric Age is transitioning beyond the military to incorporate a wide spectrum of organizations, agencies, coalitions, and enterprises. NexNet is a concept that can meet this need, either perceived or actual. At the 10th International Command and Control Research & Technology Symposium (ICCRTS), some authoritative speakers sounded the call for developing potential solutions to this gap in capability.¹⁸ If we are ever going to be able to solve the C2 gap that could bring about self-organizing application of power sources, we must first acknowledge the essential need for executing C2 at a level above the military. In a previous paper on this subject, I described this area of C2 as “poly-discipline”...where sources of national, coalition, and non-government power

¹⁷ Alberts, David S., and Hayes, Richard E., Campaigns of Experimentation, Command and Control Research Program, March 2005, pp. 177-178.

¹⁸ 10th ICCRTS, 15 June 2005, Plenary Address, Mr. Donald Diggs, Director C2 Policy, Office of the Assistant Secretary of Defense (OASD)/NII.

operate together on a routine basis, plan together, and then execute operations in a synergistic application of power against common adversaries and common threats.

Following this line of thought to the next logical step, we can clearly see the need for an entity at the “Poly-Discipline” level to develop and manage the NexNet into reality. Beyond the standard acquisition process¹⁹, a mandate for NexNet should originate at the Federal level, bringing to bear the full authority of the Office of the President of the United States and international counterparts. As such, it is conceivable that a new innovation in C2 management at a higher level is called for. Such an agency or entity could be “The United States Command and Control Agency”, or “The International Command and Control Agency”, whose specific tasks would include maintaining the operation, access, and procedures for employing the NexNet C2 Environment.

Summary and Capture

As our world community continues to be more interconnected at every level, including societal values, economy, security, and communications, the notion that an event in one part of the planet affects those in the other parts is becoming more salient each day. In an era where information drives developmental processes, and action on that information demands coordinated response, the need for a vehicle to enable that application of the instruments of national and international power is ever more important. This paper describes a conceptual Command and Control environment whereby nations and groups of nations can effectively collaborate and coordinate the application of power to resolve military, political, and natural crises. The Latin words “Fortis Adnexus” provide the meaning of the need...*a strong, powerful, and robust connection*. The NexNet concept builds on this idiom to portray a Command and Control environment that emerges from traditional military C2, to a higher plain of thought, one that incorporates the power sources of government agencies, military forces, non-government agencies, and international agencies and coalitions. By itself, NexNet remains just a concept, but applying critical thought and socializing the requirement for such an entity may bring about a divergent change in thinking about Command and Control. This paper attempts to convey that this change is inevitable...that the solution bound in Network-Centric principle will emerge as a matter of course, but with direction and purpose the concept of NexNet can be propelled into reality.

¹⁹ Includes developing a Mission Needs Statement (MNS), Operational Requirements Document (ORD), Capabilities Development Document (CDD), Capabilities Production Document (CPD), and associated system certifications, as defined in DoD Acquisitions Process Documents.

About the Author: Mr. Oppelaar retired from the USAF with over 23 years of experience in command and control, having commanded and operated ground radar systems, AWACS, JSTARS, Aerospace Operations Centers (AOC), and NORAD Systems. He is a recognized expert in AOC operations and has been a lead instructor at the USAF's Joint Command and Control Warrior Advanced Course at Hurlburt Field, Florida. Mr. Oppelaar lead the design effort for the US Missile Defense System Safety Program and designed the Joint National Integration Center's (JNIC) Automated Health & Status System presently in use. His previous works on Synaptic Quantum Architectures and Transactional Command Authorities have been published by the DoD Command and Control Research Program (CCRP), Washington D.C. Mr. Oppelaar is currently a Senior Systems Engineer supporting development of the Deployable Joint Command and Control System (DJC2).

Disclaimer: The views presented in this paper are strictly those of the author and do not represent the official position of the L-3 Communications-Titan Group, Inc., nor any agency or entity of the United States Government.

