REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)* 23-10-2006	**2. REPORT TYPE** FINAL	**3. DATES COVERED** *(From - To)*

4. TITLE AND SUBTITLE

JOINT TASK FORCE-GLOBAL NETWORK OPERATIONS:

THE SUPPORTED COMMAND

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Kenneth S. Helfrich, LtCol USMC

Paper Advisor (if Any): N/A

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

The recent information and technology revolutions along with a few of their by-products such as the Global Information Grid and the Net-Centric Warfare Concept have brought about great changes for our nations government and military. Along with these changes are additional challenges in processes and development of command and control structures. In this paper, the present Supported and Supporting relationship between the Joint Task Force-Global Network Operations and the other Combatant Commanders is analyzed from four different perspectives. Finally, the paper draws conclusions based on the analysis and makes recommendations to adjust the command and control architecture to better protect the Global Information Grid from the ever present electronic enemy.

15. SUBJECT TERMS
JTF-GNO, Supported Command

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Chairman, JMO Dept
a. REPORT UNCLASSIFIED	**b. ABSTRACT** UNCLASSIFIED	**c. THIS PAGE** UNCLASSIFIED		16	**19b. TELEPHONE NUMBER** *(include area code)* 401-841-3556

NAVAL WAR COLLEGE
Newport, R.I.

JOINT TASK FORCE – GLOBAL NETWORK OPERATIONS; The Supported Command

by

Kenneth S. Helfrich

Lieutenant Colonel, USMC

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the "Joint Military Operations Block."

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: **__________________________**

23 October 2006

Contents

ABSTRACT

The recent information and technology revolutions along with a few of their by-products such as the Global Information Grid and the Net-Centric Warfare Concept have brought about great changes for our nations government and military. Along with these changes are additional challenges in processes and development of command and control structures. In this paper, the present Supported and Supporting relationship between the Joint Task Force-Global Network Operations and the other Combatant Commanders is analyzed from four different perspectives. Finally, the paper draws conclusions based on the analysis and makes recommendations to adjust the command and control architecture to better protect the Global Information Grid from the ever present electronic enemy.

INTRODUCTION

Throughout the ages, military powers have often taken traditional approaches towards the development of their warfighting capabilities, skills, with the inevitably of fighting their nation's wars. Recognizable periods of great change during the past two centuries have been identified as "revolutions," i.e. the scientific, the industrial, the technological, and even the informational, to mention a few. But, these revolutions have caused man to question these traditional approaches to capitalize on the changes that have been made.

> What we are seeing, in moving from the Industrial Age to the Information Age, is what amounts to a new theory of war: power comes from a different place, it is used in different ways, it achieves different effects than it did before. During the Industrial Age, power came from mass. Now power tends to come from information, access, and speed. We have come to call that new theory of war network-centric warfare. It is not only about networks, but also about how wars are fought—how power is developed.
>
> Vice Admiral (Ret.) Arthur K. Cebrowski
> Director, Office of Force Transformation
> IEEE Spectrum, July 2002

Reviewing this emerging concept of Network-Centric Warfare and what process improvements have been made to meet the challenges of this new concept will provide a map to our Military and Government to help us meet the challenges that lay ahead.

When considering this new "theory of war" suggested by Admiral Cebrowski, one very important consideration, yet an exceptionally difficult concept to grasp is how to command and control (C2) it. The Network-Centric construct supporting this new "theory of war" cuts across all levels of command, at all levels of war, and in multiple dimensions. It is obviously global, and you wouldn't be wrong to call it universal. To complicate the situation even more, some people view the network as a new weapon system, while others see it only as a system that enables the warfighter. This difference in opinion brings with it many diverse issues that can influence the ultimate decision on the C2 structure. Another consideration is that the overarching concept of Net-Centricity breaks many of the traditional paradigms of military decision making. Our future depends on a thorough evaluation and eventually, the proper application of new concepts, ideas, and open approaches to its development, implementation, use and direction.

"Warfare is about human behavior in a context of organized violence directed toward political ends. So, network-centric warfare (NCW) is about human behavior within a networked environment. "The network" is a noun, and the information technology can only be the enabler. "To network" is the verb, the human behavior, the action, and the main focus. So, implementation of NCW must look beyond the acquisition of the technical enablers to individual and organizational behavior, e.g., organizational structure, processes, tactics, and the way choices are made. In other words, all elements of the enterprise are in play."[1]

The issue at hand today is our present approach to fighting and defending our global information grid (GIG), which is the backbone to Network-Centric Warfare. More specifically, should Joint Task Force – Global Network Operations (JTF-GNO), a joint task-organized command under the authority of United States Strategic Command (USSTRATCOM), be the supported command? In situations dealing with the defense of the network, should the Military take a traditional approach and give the authority to the Geographic Combatant Commanders, or take a new approach and give the authority to the JTF-GNO?

How we presently fight and defend the GIG is through traditional concepts, via levels of command and levels of war, which will leave us vulnerable to the future cyber threats.

[1] Admiral A. K. Cebrowski, *The Implementation of Network-Centric Warfare*, Office of Force Transformation, OSD, Washington DC., Spring 2005, 1

This last decade, our government has seen a revolution in information systems and in how we do business with the network as an enabler or a weapon system. A revolution in process development and thinking will be required to properly assign authorities in the future execution of cyber warfare. Our joint military leadership must capture this innovation to leap beyond our present and dated traditionalist paradigm. The new and evolving paradigm would call for the geographic combatant commander to play a supporting role in functional areas of the Global Area of Network Operations.

BACKGROUND

To understand some subtleties of commanding and controlling the GIG, let us review the past 20 years and a couple of developments that have taken place. This will help explain the predicament we face today.

First consider the Joint Task Force-Global Network Operations command. Since the early 1990s, the Department of Defense (DoD) has worried about the threat posed to its myriad computer systems by malicious outside intrusion. Since 1995, DoD systems have been attacked up to 250,000 times a year. In 1998, the DoD established its first unit to combat cyber threats, which was known as Joint Task Force-Computer Network Defense (JTF-CND). JTF-CND was later assigned to the U. S. Space Command in 1999. Several years later in April, 2001, U.S. Space Command was the additional mission of computer network attack (CNA). The Joint Task Force was then renamed the JTF for Computer Network Operations (JTF-CNO).[2]

After Space Command and its mission was rolled up into United States Strategic Command, JTF-CNO was designated as the Joint Task Force – Global Network Operations

[2] Colin Robinson, *Military and Cyber-Defense: Reactions to the Threat*, Terrorism Project, Center for Defense Information, 8 Nov 2002, http://www.cdi.org/terrorism/cyberdefense-pr.cfm (accessed 28 Sept 2006).

(JTF-GNO). The JTF-GNO was then given the mission to direct the operation and defense of the Global Information Grid across strategic, operational, and tactical boundaries in support of the DoD's full spectrum of war fighting, intelligence, and business operations. Now we have USSTRATCOM, a Functional Combatant Command (COCOM), through the JTF-GNO, directing the daily operation and defense of the GIG.

Another development that is balanced against USSTRATCOM being a Functional COCOM, is that the network has become global; crossing the boundaries of all other functional and geographic combatant commands. Each of these commands will exercise their overall authority within their assigned regional area of the world. The Unified Command Plan is the document that provides guidance and missions for all the COCOMs, establishing the Area of Responsibilities (AOR) for each of the Geographic COCOMs and specifying functional responsibilities of the Functional COCOMs. Any event happening around the world that could impact the United States, will occur in one of the five regionally assigned parts of the world, and therefore be a responsibility of a Geographic COCOM. But, if an event involves any part of the Global Information Grid, it will also fold into the functional responsibilities of JTF-GNO. Here lies the problem that only an untraditional approach, an innovation in C2 structure that will bring us closer to reaching our maximum capabilities in the realm of cyber warfare.

In an attempt to make this work amongst the community of networks operations (NETOPS), the Commander of USSTRATCOM published a concept of operations (CONOPS). This NETOPS CONOPS is a DoD directive and applies to all the Military Services, Combatant Commanders, Agencies, and all users of the GIG. Network Operations face the same set of hierarchical C2 complexities as any other joint force operation. To facilitate net-centricity, NETOPS must adopt new Information Age C2 structures and processes that breed self-synchronized support for effective operations and defense of the GIG.[3]

Analysis

"For centuries, the military has debated the pros and cons of command centralization or decentralization. Centralization promotes operational efficiency by concentrating resources and lowering transaction costs; coordination becomes a many-to-one rather than a many-to-many problem. Decentralization promotes allocative efficiency by letting users expend scarce resources on their most pressing problems. It promotes flexibility by permitting all users to adapt their information requirements to their own needs."[4]

The background of the JTF-GNO and US Strategic Command covered earlier helps explain where the JTF-GNO is today with its relationship amongst the other Functional and the Geographic Combatant Commanders. Why the C2 relationship between the JTF-GNO and the Geographical COCOMs needs to change and the direction we should head in the future can best be explained if analyzed from four different angles.

Using operational factors, attack angle one can basically be stated as the compression of the of time, space, and forces with respect to cyber warfare. Warfare at all levels is to take and maintain freedom of action. It is also the ability to carry out critical and diverse decisions in a timely manner in order to accomplish military objectives. Throughout history, all great military leaders had a natural ability to evaluate the factor of space, the strengths and weaknesses of their own forces, and the speed of their own movement. Freedom of action is achieved primarily by balancing the factors of space, time, and forces. These factors and

[3] U.S. Strategic Command, *Joint Concept of Operations for Global Information Grid Network Operations*, Offutt Airforce Base, NE, 4 August 2006, 11
[4] Martin Libicki, *Who Runs What in the Global Information Grid*, Rand, Santa Ana, Ca, Copyright 2000,11

how each is impacted by the ever increasing world of information are critical for making decisions at all levels. The higher the level of war, the more critical these factors are.[5]

Not only is information becoming increasingly a decisive combination with respect to the factors of time, space, and force, but evidence suggests that information and its network compresses the factors of warfighting. The time it takes electronic information to travel around the world, across levels of war, through multiple COCOM boundaries, including the boundary of space is measured in seconds or less. The time it takes an adversary or terrorist to attack one computer or multiple systems of computers is only a matter of seconds. With the factor of time being compressed to mere seconds, we can not afford to lose time trying to determine who has responsibility to act first or most importantly, lead.

In terms of the cyber battlefield, the factor of space has grown enormously. Every additional system, sensor, satellite, and computer that is virtually connected to GIG automatically increases the size of the battlespace accordingly. Firewalls, routers, switches, and software can create obstacles for the enemy, but our military systems that are 14,000 miles away are basically as close to the enemy as the system that is right next door. With respect to time, the globe for all practical purposes is much like a regional AOR for USSTRATCOM – it just so happens to be a very large region.

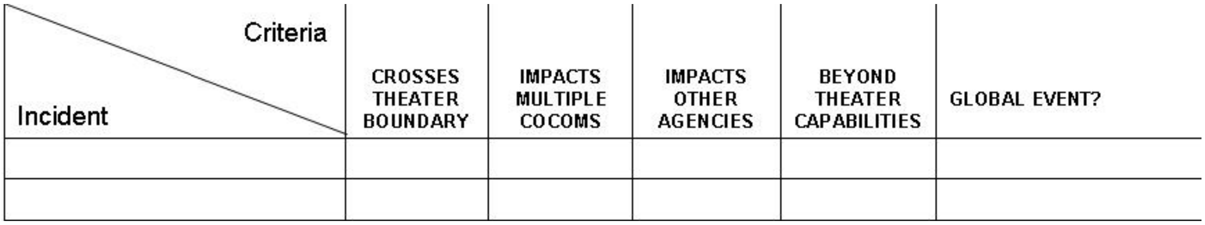
Force is the third factor to consider. This factor is probably the one we have the most physical control of, while having the smallest impact. The delta of both time and space factors have increased exponentially, based on the speed of electrons and the improvements of technology beyond our attempts to control it. But the factor of force can be mitigated to some degree. Ways we can minimize the delta in the force factor is personnel, training, equipment, and processes. Personnel, training, and equipment, to a large degree, can be dealt

[5] Milan Vego, *Operational Warfare*, Naval War College, Copyright 2004, 29

with fiscally. Processes will be the most difficult to handle, and can only be dealt with through change that is consistent with the changes in cyberspace. We must view the speed of change in information technology as an enemy to itself. We have to anticipate its future and develop processes in order to stay ahead and in control as opposed to reacting to it.

A second angle looking at the C2 relationships of the GIG and the need for a change is unity of command. The purpose of unity of command is to ensure unity of effort under one responsible commander for every objective. Unity of command means that all forces operate under a single commander with the requisite authority to direct all forces employed in pursuit of a common purpose. Unity of effort, however, requires coordination and cooperation among all forces toward a commonly recognized objective, although they are not necessarily part of the some command structure. Unity of effort – coordination through cooperation and common interest – is an essential complement to unity of command.[6] The need for Unity of command is necessary to prevent any gaps or seams in the leadership structure, and therefore possible gaps in the global network.

The present procedures and guidelines that set the C2 hierarchy during an attack or event on the GIG are illustrated below:



Criteria Incident	CROSSES THEATER BOUNDARY	IMPACTS MULTIPLE COCOMS	IMPACTS OTHER AGENCIES	BEYOND THEATER CAPABILITIES	GLOBAL EVENT?

- The direction of operations and defense of the GIG shall use supporting/supported command relationships. These relationships may be defined at the strategic, operational, and tactical levels to include all CC/S/As.

[6] Chairman, U.S. Joint Chiefs of Staff, *Joint Operations*, Joint Publication 3-0 (Washington, DC: CJCS, 17 September 2006, A-2.

> • The supported commander has the authority to take whatever NetOps action is deemed necessary, to support the mission and has final decision responsibility.[7]

Based on this chart and what is presently understood by the Geographical COCOMS is that an event or small number of events that occur within their AOR initiates a C2 structure of defense and designates them as the supported command. JTF-GNO and the other COCOMS then take a supporting position to assist the "infected" geographic COCOM. Once the network attack/event breaks the boundaries of at least two global regions, JTF-GNO would then take the helm as the supported command. To reiterate, unity of command is to ensure unity of effort toward a common objective. Events that interfere with the objectives to operate and defend the GIG, both operationally and strategically, are global in nature. This places the JTF-GNO in the best position to lead the effort.

A geographic COCOM defending against a localized enemy network attack is basically a tactical approach to an operational or strategic problem. Even though the attack can be pinpointed to a location within the COCOMs AOR, the attacker could be anywhere in the world. Time spent by the geographic COCOM making tactical maneuvers is time lost for the operationally/strategically positioned JTF-GNO to engage early as the lead force. With a global perspective, the JTF-GNO can make changes and adjustments in all AORs to mitigate any impact on the GIG.

Some Service Network and Operations Security Centers (NOSC), the Navy for example, have considered themselves as being the "supported" command, since their command would have the most direct affiliation with the attack and the remedial action taken to mitigate it. They believe neither the Geographic nor Functional COCOMs being the

[7] U.S. Strategic Command, *Joint Concept of Operations for Global Information Grid Network Operations*, Offutt Airforce Base, NE, 4 August 2006, 12

supported commander, but they see their Service NOSC in control and therefore should be the supported commander.[8] But this action/thought process would take us even further from the target. It too, would bring actions down to the tactical level, and to a lower level of command.

The development of truly Joint Forces is the third attack angle to redefine the C2 roles in the defense of the GIG.

> While technology has provided the military with dramatically improved warfighting capabilities, fully realizing and exploiting these capabilities requires that future forces become more inherently joint. They must be born joint. They must be network-centric and capable of seamlessly integrating to form a combined-arms, dominant-maneuver force that thinks and acts as one. Future operations will be characterized by light, mobile, networked forces moving rapidly and simultaneously from several different axes in a widely distributed theater of operations; lethal attacks on selectively engaged targets with high probability of success; fewer casualties and less collateral damage; and a better-informed force able to prosecute war at higher levels of effectiveness and lower levels of violence. With the technologies available today, as well as those on the near horizon, the net-centric, dominant-maneuver forces envisioned in Joint Vision 2020 are within reach. These technologies will enable the military to act with greater speed, agility, and a more measured and precise lethality; however, they will also dramatically complicate battlespace command and control.
>
> The fundamental challenges facing the command and control of a net-centric, dominant-maneuver force are related to two broad areas: communications technology and C2 doctrine or philosophy. First, a net-centric force would require a fast, reliable network that is secure and accessible to all participants in the battlespace. Second, the C2 architecture and procedures used by these net-centric forces must be rapidly responsive to changes and fleeting opportunities within the battlespace. Ultimately, to obtain and sustain information superiority, and to achieve dominant maneuver, the myriad activities and communications taking place within the modern battlespace must be constantly integrated and acted on in real time.[9]

The fundamental challenge mentioned here of C2 doctrine and philosophy is completely intertwined with the other challenge of communications technology. This challenge can be

[8] Captain Carlene Wilson, USN, Discussion, 3 Oct 2006

[9] Paul Dolson, *Expeditionary Airborne Battlespace Command and Control,* Joint Forces Quarterly, 3rd Quarter 2005, 68-75

met with large defense budgetary adjustments to stay on the future's cutting edge, just ahead of the enemy. But, this will only be possible if it is tempered with clear vision and direction; a holistic and interoperable approach to global network security. This vision and direction for the GIG must come from one source alone, not from the 4 service chiefs or the 5 geographic COCOMs who have their own budgets and competing priorities. It must come from an untraditional source; the one that know the network best and that has the mission to operate and defend it. Once again, this untraditional source is the JTF-GNO.

The fourth and final attack angle is the review of commercial network business practices. Even though military and commercial requirements may differ at times, the military has a lot to learn from the business practices of enterprise commercial network security. Many of the systems and software the military use today are from the commercial industry and their process can be applied respectively.

Actions recently taken by the commercial provider Global Crossing are an example of consolidating control of a very wide and diverse networkl. Historically, Global Crossings organization had been fragmented with many departments responsible for their own security. Their corporate leaders recognized that the convergence of all security matters under one department was necessary to obtain a complete understanding of the threats to the company's assets, personnel, and intellectual property. In 2002, *Global Crossing* pioneered a converged security philosophy and a strategic plan for protecting its infrastructure through a comprehensive defense-in-depth approach transcending physical and logical security. The success of the converged security approach has depended upon centralization, policy, command, and uniform use of technology.[10]

[10] Michael Miller and Paul Kouroupas, *Securing the Global Enterprise,* Security Technology and Design, April 2006, 22

Global Crossing was successful at securing their global enterprise by centralizing all security functions under one officer. This consolidation ensured consistent application of security measures throughout the organization. This also set the universal standards to best secure the enterprise; requiring uniform use of technology and applications throughout the corporation and ensuring interoperability.

"Believe it or not, best practices in network security begin with a top-down policy. Policy begins with understanding what it is you need to protect and what it is you need to protect against. Levels of responsibility need to be understood that implies security is everyone's job; as each employee understand how he or she contributes to the organization. Best practices in network security are more about the *what* and *why* of securing the organization's information assets than about the *how*."[11]

Another example of a commercial company applying quality business practices of enterprise network security is *StillSecure*. This company views network security as a mission-critical concern for enterprises, government agencies, and organizations of all sizes. *StillSecure* takes a layered approach to securing its network. The layered approach is seen as a technical strategy espousing adequate measure be put in place at different levels within the network infrastructure. It is also viewed as an organizational strategy, requiring buy-in and participation from the board of directors down to the shop floor.[12] The most important thing to point out here is the organizational strategy. It is this organization strategy, or the command and control relationship that is the issue; the top-down, across the board buy-in required to execute such a strategy.

[11] Marcia J. Wilson, *Network Security: Best Practices*, Computer World Security, 27 January 2003, http ://www.computerworld.com, (accessed 23 September 2006)

[12] Mitchell Ashley, *Layered Network Security 2006: a best practices approach,*StillSecure White Paper, Jan 2006, https://www.latis.com.docs.StillSecure_LayerSecurity.pdf, (assessed 16 Oct 2006)

Finally, having analyzed the C2 issue from four different perspectives (warfighting factors, unity of command, joint influences, and commercial business practices), it should be noted that in the process of reviewing commercial practices there was a common denominator with their approach to enterprise network security. This common denominator is a layered security approach. It was a reoccurring theme to be used in nearly every corporative network strategy reviewed and is applicable to some degree to the final C2 recommendation of the Global Information Grid. More specifically, the purported best practice for Symantec, Windows, Nortel, and others was that of securing the network with layers of Intrusion Prevention, Firewalls and Virtual Private Networks, Web and Email, and Anti-Virus protection, which are further applied at the given security levels (Data, Host, Application, Network, and Perimeter). This layered security approach is best enabled through centralized command and decentralized execution; basically, an organizational strategy to orchestrate the operation and the execution of a diverse defense in depth of the global information grid.

This centralized command and decentralized execution of the layered defense of commercial networks bring us back to the very beginning of our analysis, and their respective pros and cons. The layered defense supports a case for centralized control or global management to fill responsibility and authority gaps, achieve interoperability and information coherence, while at the same time supporting the case of decentralized execution, enabling the user to control some level of their own destiny.

CONCLUSION

DoD’s organizational schema (vertical/Napoleonic) is based primarily on “Industrial Age” tenets where people and things occupy geographic footprints to execute the mission of a commander. As you know, NETOPS and the GIG defy this model in their need to remain global and exist without boundaries.[13] Traditional approach will not work – it will require the use of ART to develop the proper support relationships between the functional and geographic commander.

> Innovation - Joint Vision 2010 identified technological innovation as a vital component of the transformation of the joint force. Throughout the industrial age, the United States has relied upon its capacity for technological innovation to succeed in military operations, and the need to do so will continue. It is important, however, to broaden our focus beyond technology and capture the importance of organizational and conceptual innovation as well. Innovation, in its simplest form, is the combination of new "things" with new "ways" to carry out tasks. In reality, it may result from fielding completely new things, or the imaginative recombination of old things in new ways, or something in between. The ideas in JV 2010 as carried forward in JV 2020 are, indeed, innovative and form a vision for integrating doctrine, tactics, training, supporting activities, and technology into new operational capabilities. The innovations that determine Joint and Service capabilities will result from a general understanding of what future conflict and military operations will be like, and a view of what the combatant commands and Services must do in order to accomplish assigned missions.[14]

Doing new "things" in new "ways" must be the ART of our future policy and doctrine development in the net-centric environment. Our efforts must be to reach beyond technology capturing the importance of organizational and conceptual innovation. We will need to consider what military information and their networks should be a global responsibility and what should be local? A global approach will enhance coherence in the information domain, while a local approach will ensure a tight fit between the supply and demand for information. We must work toward a strategy of "centralized architecture, decentralized services."[15]

[13] Lieutenant Colonel Steve Mayhew, USA, JTF-GNO J5, email 22 September 2006
[14] Joint Vision 2020, US Government Printing Office, Washington, DC, June 2000, 10
[15] Martin Libicki, *Who Runs What in the Global Information Grid*, Rand, Santa Ana, Ca, Copyright 2000, 41

One final observation of the situation; if one were to lay templates of centralized architecture, unity of command, and commercial business practices over the present Command and Control architecture for the GIG, it would be readily apparent that the DoD is 90 percent on-target. The 10 percent off-the-mark, and still needing adjustment toward a clearer future, falls into the definition of supporting and supported commander. Based on the analysis of the "supported and supporting" issue from the four previous angles, computer events are global in nature, and the JTF-GNO should be the supported command. The Geographic Combatant Commanders will always have the ability to protect their own networks, but the JTF-GNO must be the supported commander to best defend the Global network.

RECOMMENDATION

"First, there must be a strong bias toward interoperability with DoD, reflected not only in Pentagon decision making on programs by also through the creation and enforcement of supporting architecture. This bias is already emerging; it need to be strengthened."[16]

The elusive nature of adversaries and the ever increasing speed of global communications and the media demand greater adaptability and networking from US Joint Forces, particularly communications and intelligence resources. Consequently, the US Military conducts some operations on a global, not theater, scale e.g., network operations, space control). These operations are conducted in depth, focusing on the threat source across

[16] Martin Libicki, *Who Runs What in the Global Information Grid*, Rand, Santa Ana, Ca, Copyright 2000, 43

geographical regions that include forward regions, approaches, ad the homeland and the Global Information Grid (GIG).[17]

If we do not set a new course, we will be doomed to execute tactical combat maneuvers on the operational and strategic battlefields of the global information grid. It can be said tactical errors can create operational or strategic effects. With the GIG in mind, if we do not put the properly positioned and most capable authority in charge as the supported commander, any one of the endless and numerous attacks on the GIG throughout the world and its five geographic combatant commands could result in unexpected strategic effects.

Network Operations faces the same set of hierarchical C2 complexities as any other joint force operation. To facilitate net-centricity, NetOps must adopt new Information Age C2 structures and processes.[18] The Network Operations Concept of Operations for the JTF-GNO should clearly state that events on the Global Information Infrastructure are inherently Global and that the JTF-GNO will have the responsibility to deal with these events as the supported command. Any other command relationship will leave a seam or a gap in the security of the network that an enemy can capitalize on. Even when the JTF-GNO is the supported command, all other actions taken at any level of command or any level of warfare, are all still in concert with the efforts of the JTF-GNO; for their mission is the daily operation and defense of the GIG.

[17] Chairman, U.S. Joint Chiefs of Staff, *Joint Operations*, Joint Publication 3-0, Washington, DC: CJCS, 17 September 2006, I-15

[18] U.S. Strategic Command, *Joint Concept of Operations for Global Information Grid Network Operations*, Offutt Airforce Base, NE, 4 August 2006, 10-11

SELECTED BIBLIOGRAPHY

Ashley, Mitchell, *Layered Network Security 2006: a best practices approach,*StillSecure White Paper, Jan 2006, https://www.latis.com.docs.StillSecure_LayerSecurity.pdf, (assessed 16 Oct 2006).

Cebrowski, A. K., *The Implementation of Network-Centric Warfare*, Office of Force Transformation, OSD, Washington DC., Spring 2005.

Chairman, U.S. Joint Chiefs of Staff, Joint Operations, Joint Publication 3-0 (Washington, DC: CJCS, 17 September 2006.

Department of Defense, U.S. Strategic Command, *Joint Concept of Operations for Global Information Grid Network Operations*, Offutt Air Force Base, NE, 4 August 2006.

Dolson, Paul, *Expeditionary Airborne Battlespace Command and Control*, Joint Forces Quarterly, 3rd Quarter, 2005.

Joint Vision 2020, US Government Printing Office, Washington, DC, June 2000.

Martin Libicki, *Who Runs What in the Global Information Grid*, Rand, Santa Ana, Ca, Copyright 2000.

Mayhew, Steve, LtCol USA, JTF-GNO J5, email 22 September 2006.

Miller, Michael and Kouroupas, Paul, *Securing the Global Enterprise*, Security Technology and Design, April 2006.

Robinson, Colin, Military *and Cyber-Defense: Reactions to the Threat*, Terrorism Project, Center for Defense Information, 8 Nov 2002, http://www.cdi.org/terrorism/cyberdefense-pr.cfm (accessed 28 Sept 2006).

Wilson, Carlene, Captain USN, Discussion, 3 Oct 2006.

Wilson, Marcia J., *Network Security: Best Practices*, Computer World Security, 27 January 2003, http ://www.computerworld.com, (accessed 23 September 2006).

Vego, Milan, *Operational Warfare*, Naval War College, Copyright 2004.