3

(b)(4)

December 30, 2006

# ORGANIZING NETWORK CENTRIC WARFARE:
## Information Overload and U.S. Naval Oversight

## FINAL REPORT, OPTION YEAR TWO

by

Dr. Adam N. Stulberg
Dr. Michael D. Salomone

Michael D. Salomone, Ph.D., Project Director

*"The views, opinions, and findings contained in this report are those of the authors and should not be construed as an official Department of Defense position, policy, or decision."*

*Prepared for:*

**The Director**
**Office of the Secretary of Defense**
**Net Assessment**

(b)(4)

# *JOINT MANAGEMENT SERVICES, LLC*

(b)(6)

## Table of Contents

# ORGANIZING NETWORK CENTRIC WARFARE:

## Information Overload and U.S. Naval Oversight

### Executive Summary

This project assesses systematically the contemporary issues, debates, and proposals for crafting optimal organizational forms for network centric warfare (NCW) and for forging common knowledge towards these aims within the US. Navy. To date, transformation to NCW has been frustrated by uncertainty over two dimensions to organizational change. The first centers on debate over the capacity of organizations to realize new possibilities for near-instantaneous collection, analysis, dissemination, and precision strike provided by the information revolution. NCW enthusiasts argue that new technologies augur well for securing unprecedented information superiority, shared awareness, flexibility, speed of command, and self-synchronization that will enable the US Navy to increase by orders of magnitude new sources of power, efficiency of command and control, performance on the battlefield, and overall policy effectiveness. At the crux of the argument are assumptions that more and better information translate directly into useful information for command and control, and that networked structures dramatically accentuate effective decision-making.

By contrast, the critics question the utility of new information technologies, arguing that near-simultaneous access to "more and better" information exacerbates organizational friction to the detriment of effective service decision-making and performance. In particular, NCW risks exciting organization pathologies associated with information overload, simultaneous decision-

making, bounded rationalities, and satisficing. However, a close reading of organizational theory suggests that both perspectives are problematic, with the former understating and the latter overstating the challenges of managing organizational uncertainty. This "dialogue of the deaf" on service decision-making is a function of mutual neglect of the effectiveness of different organizational designs and procedures for delegating and overseeing the processing and analysis of information.

A second element of uncertainty pertains to understandings of the operational utility of NCW within the US Navy. Notwithstanding initial progress towards crafting material and promotional incentives for embracing new "ways of war," the prospects for NCW transformation remain stymied by the lack of shared knowledge concerning the meaning and significance of NCW among officers within the service. Absent commonly accepted benchmarks, evidentiary standards and metrics for defining, evaluating, and implementing NCW, it is not clear if and how US naval officers can forge or communicate shared understandings of NCW to supervise the requisite service transformation.

The principal investigators extend previous research on organizational structures of NCW to address these two critical dimensions of uncertainty. They assess the tradeoffs of different organizational designs for bridging the gap between more, better, and useful information processing. Applying insights from Normal Accidents Theory and High Reliability Theory, the report evaluates the advantages and disadvantages of redundancy and alternative forms of oversight for managing a range of information challenges (e.g. overload vs. efficiency; duplication versus overlapping oversight; division of labor vs. simultaneous decision-making;

sequential vs. simultaneous decision-making; intrusive vs. indirect oversight; coordination of self-synchronized units vs. hierarchical supervision). This is complemented by empirical evidence of contemporary NCW developments (such as the US Navy's experience with carrier group air defense and projections for FORCENET) to generate organizational lessons and prescriptions for strengthening oversight of network centric operations. These include reliance on:

- competition among units delegated with complementary authority;
- managerial strategies of "benchmarking"
- clear delineation of authority for human-to-human interactions
- average information processing rates
- anticipated average information arrival rates.

## Introduction

In *On War,* Clausewitz notes that one of the greatest difficulties confronting military organizations relates to the collection and processing of information under both peacetime and battlefield conditions.[1] Since the central command agency is usually detached from forward deployed units and combat operations, it relies almost exclusively on the transmission of information and expertise. Accordingly, a central command must delegate authority to collect and process information so that it can accurately analyze and act on it. The concept of network centric operations (NCO) promises to ease this challenge by integrating sensor, engagement, and information grids with superior command and control processes to create a common operating picture of the battlefield that will enable commanders to respond with greater speed, precision, and synchronicity of individual units. It is assumed that underlying information technologies and systems will empower commanders both to acquire unprecedented volumes of information and intelligence, and to optimize the calculation of options and execution of decisions, under immense uncertainty and complexity, in near real time. In short, networked information systems will facilitate the emergence of integrated, loosely coupled, and "flatter" command structures that augur well for efficient, reliable, and effective decisions and operations.

The concept of NCO, however, is not without its critics. Skeptics, for example, underscore the prospective tensions that lie at the intersection of technology and organizational behavior. Though rejecting traditional characterizations of military organizations as "tightly

[1] Carl von Clausewitz, *On War* trans. J.J. Graham (New York: Barnes and Noble Books, 2004), 56-57.

coupled," they nonetheless draw distinction between new technical possibilities of information gathering, on the one hand; and long-standing organizational challenges of collecting and analytically processing information, on the other hand. The concept of NCO is presumed to falter as the introduction of novel technical solutions that feature non-linear acquisition of information and expertise outpace the requirements and capacity of military organizations to process usable information, as the latter are steeped in hierarchical supervision and linear decision-making procedures that are designed to regulate the complexity and uncertainty of the operating environment. The resulting gap between the vast amount and type of information transmitted and the cognitive and procedural limitations to simplifying and converting it into action is expected to produce problems of information overload, with deleterious consequences for military command and control. Accordingly, the prospective benefits of NCO rest with the administrative mechanisms put in place to harness new military technologies and systems to generate in real-time better and usable information for formal and informal groups working within centralized service hierarchies, rather than with transforming military organizations to function as synchronized decentralized units.

At the crux of this debate are different assumptions about the relationship between acquiring and processing information and specific design features of complex military organizations. Can technologies that enable military organizations to collect more information yield better decisions? What are the organizational design features most appropriate for exploiting new technological and knowledge possibilities for NCO? Do new digital capabilities aggravate traditional tensions between technological possibilities for information dissemination, and typically rigid administrative procedures and division of authority for conducting effective decision-making? Or, can the human-machine problem of information overload be mitigated by alternative hierarchically-designed command architectures for overseeing intra-service relationships?

In this report, we argue that both the proponents and critics are right for underscoring the importance of organizational design features for realizing the promise of NCO; but for the wrong reasons. On the one hand, NCO enthusiasts are overly sanguine about the advantages of redundancy, as manifest in characteristics of synchronized coordination, duplication and overlapping authority, and constructive competition associated with decentralized, parallel and "loosely coupled" organizational forms. They are too quick both to embrace the premise of "high reliability theory" for organizational behavior and to write off the capacity of hierarchical and centralized structures to adapt efficiently and effectively to fluid task and technology environments under certain conditions. On the other hand, the critics are excessively wedded to intrusive and top-down approaches to administrative control, and tend to overlook the benefits of administrative strategies of "benchmarking, as well as of tapping into informal and indirect management and oversight mechanisms.

In contrast to both, we argue that there is no optimal organizational design for NCO command and control; instead there are tradeoffs associated with specific forms and features of redundancy that must be acknowledged up front and that depending on certain conditions can be better suited for managing discrete NCO tasks. Specifically, these key tradeoffs are associated with specific designs that relate to the levels of duplication, overlapping versus monopoly of authority, and competition among outside players, sub-units and within the task environment.

This report explicates these issues by analyzing the strengths, weaknesses, and tradeoffs associated with alternative notional organizational design features as they interface with contemporary debates over NCO and shape the requirements for NCO offices for the U.S. Navy. The first part describes basic organizational problems of information overload that are implicated by the advent of NCO. The second part presents the fundamental issues of organizational design that lie at the heart of the debate between the proponents and critics of NCO. The third part relates this to the broader debate between "high reliability theory" (HRT) and "normal accident theory"(NAT), rendering analytical critiques of both schools. The fourth part assesses the tradeoffs associated with a specific design features, redundancy, and relates this analysis to specific examples gleaned from elements of the contemporary NCO architecture either in place or envisioned for the U.S. Navy. The final section identifies alternative conditions and managerial techniques for contending with the redundancy problem in thinking about new organizational relationships for NCO.

## Part One: Information Overload

A critical issue confronting military organizations relates to converting raw data into useful decisions and action by command authorities.[2] During the course of a campaign, lower level officers usually provide a steady stream of information through regular progress reports or material requests. Yet, as noted by Clausewitz, "a great part of the information obtained in war

[2] Michael D. Salomone and John P. Crecine, "Information-rich Environments: Organizational Design and Decision Making Issues" *Defense Analysis* 13, no. 2 (1997), 185.

is contradictory, a still greater part is false, and by far the greatest part is of a doubtful character."[3] Before information reaches the central command authority, it needs to be filtered, interpreted, and combined with other relevant data generated from subordinate but more expert agencies.[4] However, given asymmetries of information, expertise, and authority among commanders and sub-units and the attendant administrative costs in time and resources for central oversight, there are structural constraints on internal coordination. Accordingly, the amount of incoming information concerning a particular event is directly proportional to the efficiency of the effort exerted by the command staff and the length of delay in managing the information flow and acting on a situation. Thus, the most acute problem facing command and control relates usually not to the lack of information, but to the administrative mechanisms put in place to collect, analyze, and act upon it.[5]

Traditionally, too much information has proved to be detrimental for military command and control. With excessive amounts of data streaming into a command center from delegated units, the staff tends to overwork itself to keep pace, devoting the lion's share of time and resources to compiling data rather than to performing other functional duties. As discussed in previous projects (See Appendix A on successful and unsuccessful military transformations.), this intensifies traditional principal-agent problems within military hierarchies, as delegated units that are more proximate to local information and expertise face incentives to bias the information flow and minimize intrusive oversight. In addition, high levels of information flow risk overwhelming rigid organizational structures and operating procedures that are otherwise

[3] Clausewitz (2004), p. 56.
[4] Salomone and Crecine (1997), p. 185.
[5] Ibid., pp. 185-186.

designed to mitigate the uncertainty and complexity of the internal and external decision environment. The result can be information overload that can degrade the quality of decision-making. A classic example comes from the French General Headquarters (GHQ) during the German blitzkrieg attack in 1940. From the outset, the massive influx of information caused GHQ to lose track of events on the battlefield.[6] Remarking on his experience, French General Andre Beaufre noted that a flood of detailed information overwhelmed the GHQ and officers passed on sleep to address the issue.[7] Consequently, the French command made several poor decisions brought on by information overload and exhaustion that proved decisive for the collapse of the entire French defense.[8]

At the nub of the problem of information overload is the longstanding tension between organizational challenges of acquiring new and more information, and the structures and procedures designed to effectively analyze a problem and coordinate action. As the former increases -- yielding a greater range of topics that a commander must consider, more noise that must be filtered out, and competing demands for scarce decision-making resources -- it is likely to degrade the latter by decreasing a commander's attention devoted specific issues, restricting opportunities for careful analysis, and potentially initiating "a positive feedback loop of poor decision-making."[9] Research in systems engineering, for example, has found that at a certain point an organization loses the ability to process information as it enters the system and new problems arise.

[6] Ibid., pp. 187-188.
[7] Ibid., p. 188.
[8] Ibid.
[9] Mark D. Mandeles, *The Future of War: Organizations as Weapons* (Potomac Books, Inc. 2005), p. 104.

As depicted in Figure 1, there are two rates, the average arrival rate and the average service rate, whose ratio determines a system's capacity for producing an item. This ratio between them is known as the utilization rate and determines what percentage of the system is being used on average.[10] When the utilization rate exceeds 1, the system can no longer handle the influx, and an infinite queue of items waiting to be processed begins to form.[11] According to this principle, if the average information arrival rate is greater than the average information processing rate, the central command loses its ability make decisions based on the current battlefield conditions.

[10] *Modeling in Industrial Engineering,* Pearson Custom Publishing, p. 159.
[11] Ibid.

## Figure 1

**Example #1**

| | |
|---|---|
| Information Inflow | = 1.1 Items/min |
| Information Processing | = 1 item/min |

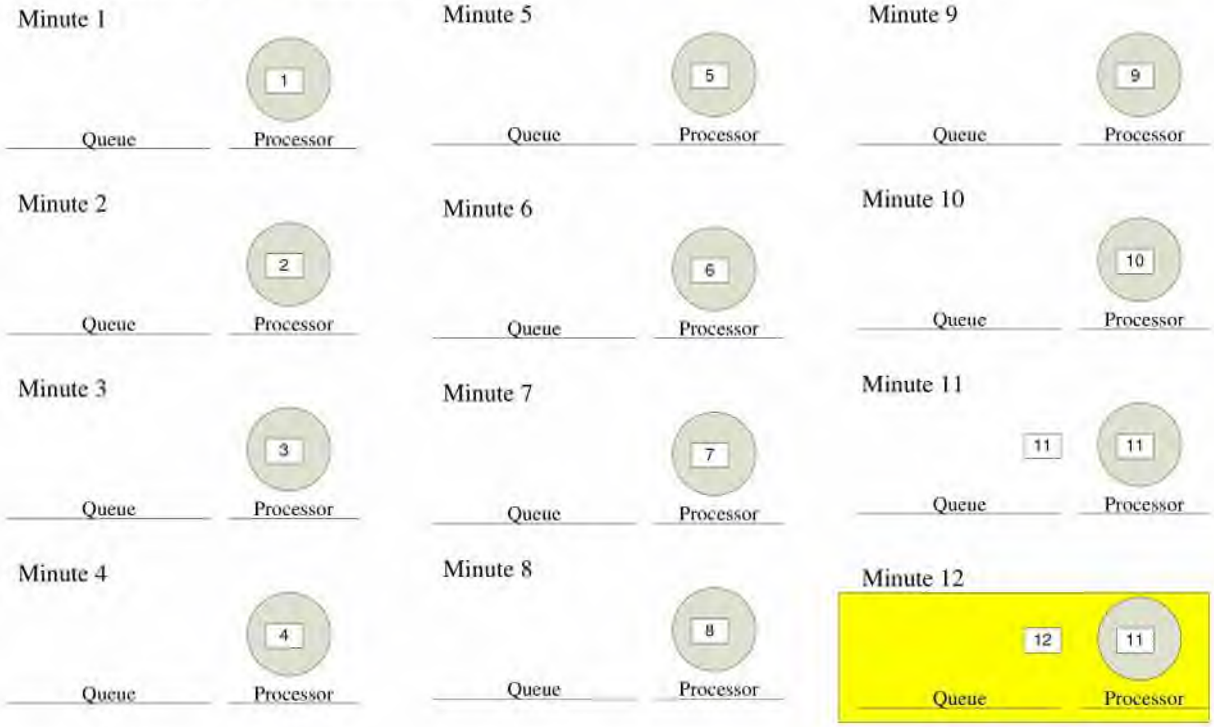

**Figure 1** **The white boxes designate pieces of information. The numbers inside the boxes correspond to their arrival sequence and the time they need to be processed by in order achieve near-real time operations. The yellow box on minute 12 denotes that the system is operating with outdated data.**

Even though the utilization rate was only slightly above 1, the system above still could not accommodate the incoming information and quickly began to process outdated data. In a military organization, this scenario would cause commanders to operate under a false reality and effectively corrupt its OODA loop by leading it to orient, decide, and act based on obsolete observations. This has lead some to conclude that: "Perhaps the greatest "fog machine" in war, as well as organizational life in general, is the overload of information."[12]

**Part Two: Organizational Design and the NCO Debate**

A major debate surrounding NCO turns on alternative organizational designs for processing vast amounts of information quickly and efficiently. Ardent advocates of the concept of NCO, including Vice Admiral (Ret.) Arthur Cebrowski and John Garstka, contend that through harnessing the power of networked technologies military forces could achieve information superiority, which would enable more effective combat operations.

> Improved command, control, communication, computer, and intelligence (C4I) and connectivity offer a commander the ability to make decisions faster, to communicate decisions faster to a wider array of forces, to direct simultaneous attacks against a wider range of adversary targets, and to secure a higher responsiveness to his intent. The increase in the speed of command will shock

[12] Salomone and Crecine (1997), p. 188.

> the adversary commanders with synchronized destructive events that rapidly foreclose their courses of action.[13]

For Cebrowski and Garstka network-centric warfare is a view of the future. This view is derived from an assessment of advances in information technology and, in particular, the efficiencies derived as information networks are expanded. As Peter Dombrowski and Andrew Ross indicate, these information networks enhance the power of geographically dispersed nodes by linking them through rapid and high volume digitized data. Networking may potentially increase, by orders of magnitude, the efficiencies of individual nodes or groups of nodes.[14]

A 2003 paper published by Vice Admiral Richard Mayo and Vice Admiral John Nathman further elaborates the vision of rapid and effective use of information coupled with near-instantaneous collection, analysis, and dissemination processes as a means of dramatically enhancing Naval warfighting capabilities.[15] FORCEnet is the architecture for network-centric warfare. Stated the authors, "FORCEnet implements the theory of network-centric warfare."[16] As indicted by the Chief of Naval Operations Strategic Studies Group, "FORCEnet is the operational construct and architectural framework for naval warfare in the information age that integrates warriors, sensors, networks, command and control, platforms and weapons into a

[13] Arthur K Cebrowski and John J Garstka, "Network-Centric Warfare: Its Origin and Future" *United States Naval Institute. Proceedings* 124, no. 1 (1998) http://gtel.gatech.edu:2146/pqdlink?index=24&did=25236401&SrchMode=3&sid=1&Fmt=3&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1150698743&clientId=30287&aid=1 (accessed through Proquest on 19 June 2006).

[14] Peter J. Dombrowski and Andrew L. Ross, "Transforming the Navy," *Naval War College Review* (Summer 2003), p. 112.

[15] Richard W. Mayo and John Nathman, "FORCEnet: Turning Information into Power," *U.S. Naval Institute Proceedings* (February 2003). Http://www.nwdc.navy.mil/Concepts/IKA/ForceNetM.aspx]

[16] Mayo and Nathman, (2003), p.1

networked, distributed combat force that is scalable across all levels of conflict from seabed to pace and sea to land."[17]

Numerous proponents of the network-centric warfare concept agree that naval, army or air force units organized into networks have major operational advantages. The network increases situational awareness of all participants.[18] All parties share a common tactical picture.[19] Networked forces can fight using new tactics.[20] Commanders in the field may consult experts across the world in real time if they encounter a difficult problem.[21] Sensor to shooter time is reduced, enabling fast action and "on site analysis" of raw intelligence from sensor display.[22] Networking enables expanded collaboration and enhances speed of command.[23] Fewer personnel, fewer platforms, and fewer suppliers are needed to perform a mission more effectively and efficiently.[24]

While the vulnerability of information systems must constantly be addressed, Cebrowski contended that the threat is exaggerated and is mostly a perceptual problem: "From the inside, one's own networks often look weak and vulnerable. The same network viewed from the

[17] Quoted in Ibid.

[18] G. Gagnon, Network-Centric Special Operations—Exploring New Operational Paradigms. *Air & Space Power Chronicles*, (February 2002); P. Stillman, Small Navies Do Have a Place in Network-Centric Warfare. *Naval War College* (Winter 2004), pp. 1-16.; and D. Alberts and J. Garstka, J., Network Centric Operations Conceptual Framework Version 2.0, Naval War College Review (2004).

[19] Stillman (2004); Lt. Gen. Joseph K. Kellogg Jr., USA in: R. Ackerman, Afghanistan Is Only the Tip of the Network-Centric Iceberg. *Signal Magazine* (April 2002).

[20] J. Garstka, Network-Centric Warfare Offers Warfighting Advantage. *Signal Magazine*. (May 2003), [ http://www.afcea.org/signal/articles/anmviewer.asp?a=235&z=6].

[21] Kellogg (2002).

[22] Gagnon (2002).

[23] Alberts and Garstka (2004).

[24] C. Wilson, Network-centric warfare: Background and Oversight Issues for Congress. *Congressional Research Service, The Library of Congress* (2 June 2004), [http://www.fas.org/man/crs/RL32411.pdf].

outside, however, could appear formidable and extremely difficult to disable."[25] The key to security is network models with flexible, redundant, and rapid reconstruction characteristics.

Similarly, Cebrowski was not troubled by the charge that the system could experience information overload. Information superiority does not necessarily mean large volumes of information. Data will be transferred according to relevance, accuracy and timeliness. Once these evaluation criteria are used "the question of overload subsides."[26] The Admiral admitted that there is a danger that the emphasis on speed may lead to hasty or ill considered decisions by commanders. But he thought this was more likely in situations where information was scarce or slow in arriving. The timely arrival of critical information will more likely prevent precipitate decisions.[27]

By contrast, the critics of NCO focus on the organizational problems of information overload. Thomas Barnett, in particular, took aim directly at the purported efficiency of networked structures. First, the speed of command attributed to NCO may actually be a liability. Speed of decision may lead to miscommunication and misperception of the enemies intent. This may be particularly dangerous when dealing with enemies who have less advanced communications systems. Second, the ambitious goal of self-synchronization may dangerously undermine the observe-orient-decide-act (OODA) loop. The goal of NCO is to reduce the time required to perform the "OO" portion through self-synchronization. But in reality the speed of

[25] Arthur Cebrowski, "Network-Centric Warfare: An Emerging Response to the Information Age," Military Technology (2003), p. 20
[26] Ibid., p. 21
[27] Ibid.

information transfer should be used to lengthen the observe-orient phases of the loop.[28] Third, NCO boasts that it will create a common operating picture that will permit greater application of the commander's intent. But Barnett is concerned that the inherent pressure for speed and self-synchronization may result in all the participants relying on a common picture "as a shared reality that is neither shared nor real." The flow of data may be so great that tactical, operational, and strategic data generates information overload. NCO asserts there will be a common operating picture. But the danger is that it will be a top-down imposed picture masquerading as an inductively achieved common picture. Barnett opined:

> What is scary about NCW's (network centric warfare) ambition is the strain it may put on commanders at various levels to integrate the commander's intent from all other commanders and not just up the chain of command. NCW promises to flatten hierarchies, but the grave nature of military operations may push too many commanders into becoming control freaks, fed by an almost unlimited data flow. In the end, the quest for sharing may prove more disintegrating than integrating.[29]

Significant concerns related to the acceptance of data during network centric operations were expressed by Admiral W.J. Holland in an article entitled, "What Really Lies Behind the Screen?" [30] He maintained that the acceptance of the accuracy of data for one problem may spill over to acceptance of all or much data as equally accurate simply because it is displayed on the same computer screens. This, in turn, compounds the problem of "blowback," whereby "bad" information not only circulated but can reduce the situational awareness and erode the clarity

[28] Thomas Barnett, "The Seven Deadly Sins of Network-Centric Warfare," *U.S. Naval Institute* (January 1999) p.3.
[29] Ibid., p.4.
[30] W.J. Holland, "What Really Lies Behind the Screen/" *U.S. Naval Institute Proceedings* (April 2003), p. 73.

within which a command authority understands its environment. [31] Holland noted that the global positioning system is a dramatic and effectively used fusion of radio data, stored data bases, satellite sensors, and computer technology to create highly accurate data that revolutionized command and control. But said Holland: "GPS carries a virus that unduly buttresses belief in the accuracy of other sensors, references and databases."[32] Because the position of U.S. forces can be so accurately displayed on a screen other data to appear on the screen may easily be attributed the same level of accuracy. Experts who are fully aware of the limitations of sensors (mechanical and human) may not be the end users of data appearing on screen in a fast paced situation.

The greatest danger of network centric decision-making is that the key discussions among relevant actors will enter around the display in front of all that are 'networked.' At this man-machine interface major coordination issues will emerge as various actors interpret the data before them. As operations become more joint, actors with very dissimilar experiences, education and training will be reacting to the data on the screen. All the relevant information will never be present. The diverse actors will bring those diverse experiences to consider ambiguous data. Accordingly, the self synchronization expected by NCO advocates may not emerge. Or an equally great danger is that the consensus is imposed by the commander of the network operation.[33]

[31] Peter D. Feaver, "Blowback: Information Warfare and the Dynamics of Coercion," *Security Studies* 7:4 (Summer 1998), pp. 88-120.
[32] Holland (2003) p.73.
[33] Ibid.

The most systemic criticism of the theory of network-centric warfare was delivered by Dr. Milan Vego, Professor of Operations at the Naval War College, in an article entitled, "Net-Centric Is Not Decisive." Even though network-centric warfare has become the "new orthodoxy" of the Navy, Vego contended that the Navy must reconsider the concept as it is not a theory grounded in empirical evidence; the focus is merely on tactics and targets. Vego admonishes the Navy to restore "the balance between strategy, operational art, and tactics-before it discovers firsthand that simply netting maritime forces will not be decisive in combat."[34]

Vego argued that NCO is a seriously flawed theory of warfare. In general, the defects are: (1) it scarcely considers the relationship between national policy and military power; (2) extensively studied Clausewitzian views on the fog of war or the friction of war are discarded; (3) the art of war is reduced to the science of war; (4) psychological and moral issues are scarcely addressed; (5) the enemy is rarely assessed and it is assumed that the enemy will be incapable of adapting to NCO tactics; (6) it is assumed the U.S. will always have information superiority; (7) the pressures for centralized command and control derived from the information architecture are heavy; (8) operational art is scarcely considered; (9) the core of NCO is tactics and targets; (10) the information architecture is designed for speed in the targeting process rather than improving decision-making objectives and tasks.[35]

Vego also was highly critical of many of the key assumptions about information processing embedded in NCO such as, information superiority, situational awareness, shared awareness, speed of command and self-synchronization. NCO advocates often emphasize

[34] Milan Vego, "Net-Centric Is Not Decisive," U.S. Naval Institute *Proceedings* (January 2003) p. 1.
[35] Ibid., p.1.

"information superiority" in quantitative terms. Although highly important, extensive and timely information is only one factor for a commander's success. Such information superiority may be of little use if it is not accompanied by sound strategy or is linked to the poor application of strategy. Vego notes

> Admiral William F. Halsey's actions during the Leyte Gulf operation in October 1944 are a classic example of a commander possessing information superiority but still making bad decisions that nearly led to a humiliating defeat by an inferior enemy force.[36]

According to Vego, there are several dangers with a concept of warfare that places so much emphasis on obtaining a complete view of the tactical situation. First, the emphasis on information superiority may lead a commander to hesitate rather than to act decisively. The concept may create a group of commanders who will not act until they have "information superiority." A second danger is that the drive for information superiority in a crisis may lead to information overload, particularly at the higher levels of command. Operational commanders may be overwhelmed by a flood of indigestible data.[37]

NCO advocates believe that netted systems will lift the fog of war. In past wars situational awareness deteriorated quickly, it would be reestablished and then it would deteriorate again. Netted systems will prevent this sequence of fog contend the advocates. Vego, however, asserted that it is not specifically the quality of information that is the cause of

[36] Ibid., p.7.

[37] Ibid., p.8

the fog of war as much as the fact that the enemy changes his will or does not act according to expectations.[38]

The most significant problem with NCO is the assertion or goal of "shared awareness." NCO advocates consider this a major attribute. The drive for shared awareness compels operational commanders to become too involved in tactical decisions at the expense of concentrating on operational or strategic issues. Such commanders can easily become so focused on the tactical picture as to miss the big picture.[39] Similarly, the emphasis on "speed of command" can easily result in unsound decision making.

A major pillar of NCO is the assertion of "self synchronization." Obviously, this is a desirable goal in command structures. The mistake NCO advocates make, according to Vego, is that they assume that since it is relatively easy to accomplish this goal at the tactical level it can be realized at all levels. But implanting a system where the commander's intent is applied at the operational or strategic level is far more complicated than just netting information systems. Detailed planning, interagency coordination and practiced task sequencing are critical elements for implanting the commander's intent.[40]

The great danger of meddling on the part of commanders at various levels of an operation is a major theme addressed by critics and skeptics. For example, Lieutenant Commander Curt

[38] Ibid.
[39] Ibid., p.9.
[40] Ibid., p.10.

Copley points out that highly developed networked systems may create the temptation of well intentioned but intrusive intervention on the part of higher level commanders:

> Each level of war is complex, and if a decision maker abandons his level even briefly to make decisions at a lower level, effectiveness will be lost. This problem is not new to warfare, but the vast amount of information that network centric operations provides raises the stakes.[41]

Similarly, Lt Colonel Gregory Roman, USAF, feared that information technology may move military command structures in dysfunctional directions:

> The seductiveness of information technology stimulates military organizational orientation towards greater centralized control and more rigid hierarchical organizations instead of the desired orientation of decentralized control and more flexible organizations.[42]

This tendency toward wresting decision authority from subordinates so apparent in NCO may be moving the U.S military away from its long held organizational advantages of flexibility toward a "heavily centralized behemoth employed by the Soviet Union."[43] Another potential danger of NCO, contended David Roberts and Joseph Smith, is that this type of intrusive oversight may "stifle the initiative of lower-echelon decision makers." Few commanders in the

[41] Curt Copley, "A Commander's Network Centric Odyssey," *U.S. Naval Institute Proceedings*, (2003) p. 59.

[42] Gregory A. Roman, *The Command or Control Dilemma: When Technology and Organizational Orientation Collide*. Maxwell AFB, Alabama: Air University Press, 1997. p.3.

[43] David W. Roberts and Joseph A. Smith, *Realizing the Promise of Network-Centric Warfare*, Joint Forces Staff College, 10 March 2003, p.12

field will have incentives or opportunities "to hone their skills in operational art." [44] Consequently, in a few years of NCO operations there will be a limited cadre of experienced commanders. Captain Chris Johnson was concerned for the traditional naval concept of accountability during network centric operations, as such systems make it difficult to discern who is in charge of a ship.[45]

## Part Three: Organizational Complexity and Coupling

Over the past 25 years, a great deal of academic work has surfaced regarding the proper techniques for managing systems in order to reliably, efficiently, and effectively address information processing challenges within organizational structures. Two schools, Normal Accident Theory (NAT) and High Reliability Theory (HRT), dominate the debate. The following discussion examines and assesses these theories in order apply the lessons learned to the emerging theory of warfare regarding Network Centric Operations (NCOs).

### *Normal Accident Theory*

In response the numerous explanations for the near meltdown at the Three Mile Island (TMI) nuclear facility, Charles Perrow published *Normal Accidents: Living with High-Risk Technologies*, which examined the origins of large accidents in various systems. Perrow gave due credit to both operator error and technological failures in producing minor incidents but

[44] Roberts and Smith (2003) p.14.
[45] Chris Johnson, "Net-Centric Fogs Accountability," *U.S. Naval Institute Proceedings*, (May 2003).

attributed larger system-wide accidents to flaws in the organizational structure. This general argument formed the basis of NAT that is premised on two core concepts. The first, *system complexity*, refers to the degree to which a system includes processes beyond linear interactions.

1) **Linear Systems** overwhelmingly involve linear interactions, which have expected and familiar sequences along with high visibility.[46] The simplicity and comprehensibility of these systems decreases the probability of major accidents because problems can be easily understood and quickly corrected.
2) **Complex Systems** generally involve several complex interactions, which have unfamiliar, unplanned, and unexpected sequences.[47] In addition, complex interactions also have low visibility and are difficult to comprehend.[48] These qualities increase the likelihood of major accidents because operators and engineers must take longer to decipher the problem, during which time it could spread.

The second core concept, *system coupling*, relates to the degree to which a system incorporates alternatives, tolerances, and slack.[49]

1) **Loosely Coupled Systems** generally allow for variances. Specifically, they have processes which are not time dependent and contain multiple pathways for items to

[46] Charles Perrow, *Normal Accidents: Living with High-Risk Technologies* (Princeton, Princeton University Press, 1999), 78. See also application to defense issues by Scott D. Sagan, Limits of Safety: Organization, Accidents, and Nuclear Safety (Princeton: Princeton University Press, 1993).
[47] Perrow (1999), pp. 78 and 88.
[48] Ibid.
[49] Ibid., p. 96.

progress to subsequent stages.[50] This inherent flexibility reduces the potential for major accidents because it allows operators and engineers to delay or reroute the process as to address an issue before it disrupts the entire system.

2) **Tightly Coupled Systems** usually contain little slack. Additionally, they have time dependent processes, which adhere to a strict sequential order (e.g. B must be produced after A), and only allow one set pathway for items to complete the entire process.[51] This overall rigidity increases the likelihood of system accidents because the individual processes cannot be altered to address potential problems.

In general, NAT looks at the organization of a system and how this in conjunction with minor incidents determines the chance of a major accident. Specifically, NAT theorists are concerned with a system's complexity and the degree to which it is coupled. The combination of these two factors plays an integral role in reducing or exacerbating the potential impact of a minor incident. As long as the system is not tightly coupled and highly complex, there exists an inherent degree of safety due to either the increased slack generated via loose coupling or the increased predictability of interactions associated with low system complexity. However, when mentioning complex and tightly coupled systems, Perrow writes:

> If the complex interactions defeat the designed-in safety devices or go around them, there will be failures that are unexpected and incomprehensible. If the system is also tightly coupled, leaving little time for recovery from failure, little slack in resources or fortuitous safety devices, then the failure cannot be limited to parts or units, but will bring down subsystems or systems. These accidents

[50] Ibid., pp. 93-94.
[51] Ibid.

> then are caused initially by component failures, but become accidents rather than incidents because of the nature of the system itself.[52]

Despite its logic, Perrow argues against adding more safety devices and event indicators because it is possible that some future accident will just bypass these as well.[53] For instance, he contends that during the TMI accident the indicator for the pilot-operated relief valve, a means for relieving pressure in the core, was itself broken.[54] As a result, even with the additional safety protocols, incomprehensible interactions from the engineers' perspective still occurred, and the accident was not averted. Furthermore, Perrow notes that complex and tightly coupled systems demand a paradoxical management style. On one hand, he contends this system needs centralization in order to address the rigidity associated with tight coupling, whereas on the other hand, it also needs to be decentralized in order to deal with the unplanned interactions that result from the system's high degree of complexity.[55] Despite this seemingly black and white thinking, Perrow maintains that the necessary hybrid management style has been repeatedly tried but without success.[56] Therefore, in NAT's view, this disparity helps set the conditions for incident propagation in complex and tightly coupled systems because using either centralization or decentralization neglects the needs of one of the systems' characteristics.

Along with the aforementioned properties, NAT also looks at the units (e.g. pieces of hardware and human operators) that comprise the system. Essentially, NAT regards nothing as

[52] Ibid., p. 330.
[53] Ibid., p. 4.
[54] Ibid., p. 21.
[55] Ibid., p. 332.
[56] Ibid., p. 41.

infallible.[57] With respect to the hardware aspect, this stance is quite reasonable because 'widgets' are designed for an approximate and finite period of use before they fail.[58] Similarly, NAT also holds a dim view of the human component. "Time and time again warnings are ignored, unnecessary risks are taken, sloppy work done, deception and downright lying practiced…it occurs in all organizations, and it is a part of the human condition."[59] Given these predispositions for error and an incompatible management structure, NAT proponents state that system accidents are inevitable. Despite the pessimism, Perrow and other NAT adherents maintain that specific organizational measures-- such as clearly delineated responsibility, open channels of communication, and effective oversight-- an organization can reduce the likelihood of turning minor incidents into major accidents.

Overall, *Normal Accidents* has proved to be extremely influential and produced a substantial amount of debate over accident causation and prevention. In sum, Perrow's work on NAT has been citied over 1000 times within the social science, humanities and scientific communities between 1984 and 2003.[60] Despite this influence, *Normal Accidents* has also received a great deal of general criticism.[61] For instance, behavioral scientist Larry Hirschhorn claims that Perrow failed to pursue organizational issues in depth.[62] Specifically, Perrow's managerial paradox for highly complex and tightly coupled systems is imaginary and that nearly 3,000 factories in United States successfully employ closely coordinated non-hierarchical

[57] Ibid., p. 330.

[58] This hardware lifespan is known as Mean Time to Failure (MTTF) and is used extensively in Industrial Engineering for modeling product flow and accounting for machine downtime.

[59] Perrow (1999), p. 10.

[60] Scott D. Sagan, "Learning from *Normal Accidents*" *Organization and Environment* 17, no. 1 (2004), pp. 15-16.

[61] This does not include differences of opinion between the Normal Accident and High Reliability Theory schools.

[62] Larry Hirschhorn, "Normal Accidents" *Science* 228, no. 4701 (1985), p. 847.

organizational structures.[63] Additionally, Hirschhorn faults Perrow for merely speculating on the potential effects DNA and genetic engineering without the same historical analysis he used to support the other case studies.[64] Similarly, sociologist Peter Rossi comments, "Perrow has shown us how the sociological imagination, skillfully used, can lead to important ideas. But now we need someone to show how valid those ideas are in actual application to hard data."[65] Even if Perrow satisfied the above shortcomings, Daniel Whitney of MIT's Engineering System's Division contends that *Normal Accidents'* conclusions could not be effectively justified because it does not provide a base case for comparison.[66] In addition to his short-sightedness, other critics simply view Perrow's analysis as flawed. For instance, a group of MIT theorists argue that *Normal Accidents* fails to address engineering solutions other than redundancy (e.g. color coding or substitution of hazardous materials) as a means of improving safety.[67] Finally, sociologist Mary Douglas considers the idea of system complexity to be ambiguous. Regarding this term, she writes:

> As a term in information theory, the degree of complexity means the number of logical entailments, "if this, then that." In that sense, the term excludes the presence of unentailed loose ends, contradictions, hidden conjunctions, and false trails. But Perrow tries to use the term to mean both complexity in this precise sense and at the same time its opposite, confusion, ambiguity, disconnectedness. The result is that he has one workable dimension and one that is so unanalyzed that it can mean anything he likes. Consequently, the analysis of a very

[63] Ibid.

[64] Ibid.

[65] Peter H. Rossi, "Normal Accidents: Living with High Risk Technologies" *The American Journal of Sociology* 91, no. 1 (1985), p. 184.

[66] Daniel Whitney, "Normal Accidents" http://esd.mit.edu/WPS /wplit-2003-01.pdf (accessed 30 May 2006).

[67] Karen Marais, Nicolas Dulac, and Nancy Leveson, "Beyond Normal Accidents and High Reliability Organizations: The Need for an Alternative Approach to Safety in Complex Systems" http://esd.mit.edu/symposium/pdfs/papers/marais-b.pdf (accessed 30 May 2006).

interesting subject and fascinating case histories is flawed, and the conclusions from the arguments are not justified.[68]

*High Reliability Theory*

As mentioned above, NAT put forth a pessimistic conclusion stating that major accidents in highly complex and tightly coupled systems are inevitable due to their organization and the natural fallacies of their components.[69] In response to this claim, scores of social scientists, organizational theorists, engineers, and industrial managers established an opposing school of thought, which contended that through the proper construction and socialization of an organization, these accidents could be prevented. The following aims to outline the HRT proposed by this school and to sum up the debate between it and NAT.

HRT argues that through special High Reliability Organizations (HROs), which are intently geared towards safety, system-wide accidents can be eliminated. Not unlike their NAT counterparts, adherents to HRT do not view humans as infallible but rather that redundant safety-oriented organizations can filter out inevitable human shortcomings.[70] The core of this argument draws on Martin Landau's pathbreaking work that challenged the assumed virtues of streamlined and efficient systems, and identified positive correlations between redundancy, duplication, and overlapping oversight with organizational efficiency, reliability, and effectiveness. This both extended and fostered complementary insights on the constructive role of parallel, competitive, and informal redundant management, as well as on theories in engineering that demonstrated

[68] Mary Douglas, "Loose Ends and Complex Arguments" *Contemporary Sociology* 14, no. 2 (1985), 173.
[69] Perrow (1999), pp. 10 and 330.
[70] Sagan (1995), p. 16.

how even unreliable components, if independently and in a parallel manner, can lead to rapid increases in overall system reliability.[71] To develop this theory, researchers analyzed the operations of several highly complex and tightly coupled systems, which have remained accident free (e.g. aircraft carriers and air traffic control).[72] Despite the different stresses and processes exhibited in these environments, theorists have identified four key characteristics that define HROs.[73]

*The prioritization of safety and reliability as a goal by political elites and the organization's leadership.* High Reliability theorists contend that the leadership of an organizational must emphasize safety and reliability for two reasons. First, safety costs money. "If political authorities and leaders are not willing to devote more resources to safety, accidents will therefore become more likely."[74] Secondly, the leadership of an organization establishes the proper values and practices that dictate the appropriate behavior for the rest of the group. Therefore, by stressing a safety oriented culture, the leadership helps ensure that the rest of the organization will accept this as its operational goal.[75] For instance, the researchers noticed that the captain of the aircraft carrier clearly instructed 'green' crewman on the importance of safety

[71] Martin Landau, "Redundancy, Rationality, and the Problem of Duplication and Overlap," *Public Administration Review* 39:6 (1969), pp. 346-358; William A. Niskanen, *Bureaucracy and Representative* Government (Chicago: Aldine Atherton, 1971); Jonathan B. Bendor, *Parallel Systems: Redundancy in Government* (Berkeley: University of California Press, 1985); Donald Chisholm, *Coordination without Hierarchy: Informal Structures in Multiorganizational Systems* (Berkeley: University of California Press, 1989); and Norman Furniss, "The Practical Significance of Decentralization," *The Journal of Politics* 36:4 (November 1974), pp. 958-982.

[72] Lee Clarke and James F. Short Jr., "Social Organization and Risk: Some Current Controversies" *Annual Review of Sociology* 19 (1993), 389; and Gene I. Rochlin, Todd R. La Porte, and Karlene H. Roberts, "The Self-designing High-Reliability Organization: Aircraft Carrier Flight Operations at Sea," *Naval War College Review* (Autumn 1987).

[73] The following enumerated terms were used verbatim; Sagan (1993), p. *17.*

[74] Ibid., p. 18.

[75] Ibid., p. 19.

and that procedures were to be broken only if safety was in question. According to these theorists, this action continually reinforces the safety-oriented culture of the organization.[76]

Regarding the influence of the elites, NAT does not entirely object to this reasoning. Essentially, it argues that safety and reliability become an organization's concerns if a system directly affects the leadership or the elites.[77] On this point, Perrow notes:

> Elites fly on airplanes all the time, and airline pilots are in high demand, well paid, and in a position to have some, though not great, influence on the operation of the system. Captains and Admirals cannot escape naval vessels and a serious aircraft incident aboard a carrier will endanger their lives. But nobody of great importance works directly in a nuclear power plant, travels aboard tankers and freighters loaded with explosive and toxic cargos, sits in the potato fields, sprayed with genetically engineered microbes, or gets very close to a huge chemical plant.[78]

Despite the inclusion of the elites, NAT argues that organizations cannot maintain the prioritized emphasis on safety as demanded by a HRO because of differing interests (e.g. job security and production quotas).[79]

*High levels of redundancy in personnel and technical safety measures.* On the issue of redundancy, HRT contends that multiple cross-checking measures decrease the likelihood of an unfavorable occurrence. Specifically, it points to the operations of U.S. aircraft carriers, wherein

[76] Rochlin, La Porte, and Roberts (1987).
[77] Sagan (1993), p. 37.
[78] Ibid.
[79] Ibid., 37-38.

officers are assigned different yet overlapping tasks. In doing so, HRT argues that this safeguards against potential problems and enables the carrier crew to determine if an element is faulty before the situation becomes critical.[80] In sum, this school sides with Jonathan Bender who noted, "duplication is a substitute for perfect parts."[81]

Unlike the matter of elites, NAT and HRT call for entirely opposite measures on this issue. Regarding technical redundancy, NAT encourages using multiple redundant measures in moderation.[82] Given that minor incidents can bypass built-in backup devices, NAT maintains that it is important to evaluate the tradeoffs between decreasing breakdown probabilities and increasing the complexity of the system. On human redundancy, this school would agree that duplication produces shoddier parts than reliance on a single individual. As we discuss below, NAT theorists are quick to point out that "unlike technical devices, humans are aware of one another and the additions of an extra guard, or pilot, or radar watcher can lead others to be less observant or responsible."[83]

*The development of a "high reliability culture" in decentralized and continually practiced operations.* In managing tightly coupled and highly complex systems, the High Reliability theorists seemed to have solved Perrow's managerial paradox. Proponents hold that HROs should operate in a decentralized manner to decrease response time for unexpected issues. According to organizational theorists Lee Clarke and James Short, "…When the going gets tough, HROs get flat…so that skill and knowledge rather than bureaucratic authority drive

[80] Rochlin, La Porte, and Roberts (1987).
[81] Bendor (1985).
[82] Sagan (1993), pp. 28; 284-289.
[83] Sagan, "Learning from *Normal Accidents,"* p. 17.

decision making."[84] However, this decentralization is only made possible through ongoing centralized training. Explaining the feasibility of this concept, theorist Karl Weick writes:

> Before you can decentralize, you first have to centralize so that people are socialized to use similar decision premises and assumptions so that when they operate their own units, those decentralized operations are equivalent and coordinated. This is precisely what culture does. It creates a homogeneous set of assumptions and decision premises, which when they are invoked on a local and decentralized basis, preserve coordination and centralization.[85]

In order to create these shared assumptions and reactions, HROs implement a strict regimen of realistic emergency simulations. Without this challenge, organizations and individual members are likely to act carelessly and outside the bounds of the centrally trained troubleshooting procedure during crisis situations.[86]

Even though the management style suggested by High Reliability theorists appears to solve Perrow's paradox, Normal Accident theorists still maintain that it is inappropriate for highly complex and tightly coupled systems. Despite the ability to spot potential problems via engineers, system architects, and simulated exercises, NAT argues that unexpected issues will continue to arise.[87] In which case, the speed associated with centrally trained decentralized operations is negated because the operators are not capable of correctly handling such situations.

[84] Clarke and Short (1993), p. 389.
[85] Karl Weick, "Organizational Culture as a Source of High Reliability" *California Management Review* 29: 2 (1987), 124; Sagan (1993), p. 23. The quote was found in Sagan's work, but it was directly quoted from Karl Weick.
[86] Sagan (1993), p. 24.
[87] Ibid., p. 41.

Furthermore, Perrow argues that the management structure called for by HRO proponents has failed on multiple occasions because it does not reflect American socio-cultural values.[88]

*Sophisticated forms of trial and error organizational learning.* HRO supporters advocate that the use of trial and error learning advances the organization's ability to manage unforeseen problems. With respect to the carrier operations, High Reliability theorists contend that many of the safety innovations incorporated into the organization resulted from the experience gained in dealing with serious incidents.[89] According to theorist Aaron Wildavsky:

> Trial and error is a device for courting small dangers in order to avoid or lesson the damage from big ones…Because it is a discovery process that discloses latent errors so we can learn how to deal with them, trial and error lowers risk by reducing the scope of unforeseen dangers. Trial and error samples the world as of yet unknown risks; learning to cope with risks that become evident as the result of small-scale trial and error, we develop skills for dealing with whatever may come our way from the world of unknown risks.[90]

NAT theorists, however, challenge this claim. In particular, they hold that that accidents often happen in highly politicized circumstances, which cause organizations to protect themselves by pointing the finger at the operators or intentionally citing erroneous causes.[91] In either case, organizations appear more eager to forget about the incident rather than learning from it. Furthermore, often incidents are misdiagnosed especially in complex systems because

[88] Ibid.
[89] Rochlin, La Porte, and Roberts (1987).
[90] Sagan (1993), p. 26..
[91] Ibid., pp. 42-43.

their causes are unclear.[92] By operating under faulty premises during the next similar incident, one could actually exacerbate its effects.

Beyond its differences with Normal Accident Theory, High Reliability Theory also holds the seeds of counterproductive organizational designs. One of the major critiques regarding HROs is that its justifying academic fieldwork was conducted on systems that were not highly complex and tightly coupled. A group of MIT researchers noted that the studies regarding HRT were performed aboard U.S. Navy carriers during peacetime operations.[93] They claimed that these inherently possess significantly more slack than combat missions, which are the trying grounds for carrier operations.[94] Regarding combat operations aboard naval vessels, Clarke and Short point to the case of Iran Air flight 655, wherein the USS *Vincennes* mistakenly shot down a civilian passenger jet during the Iran-Iraq War. In this case, a companion ship USS *Sides* correctly interpreted the situation and disengaged, but organizational failures on USS *Vincennes* allowed the disaster to unfold.[95] Clarke and Short clearly state that *Vincennes* was not a HRO, but contend that, "This case suggests combat is indeed an important variable in influencing the reliability of combat oriented systems."[96]

[92] Ibid., p. 41.

[93] Karen Marais, Nicolas Dulac, and Nancy Leveson, "Beyond Normal Accidents and High Reliability Organizations: The Need for an Alternative Approach to Safety in Complex Systems" http://esd.mit.edu/symposium/pdfs/papers/marais-b.pdf (accessed 30 May 2006).

[94] Ibid.; and Clarke and Short (1993), p. 390.

[95] Clarke and Short (1993), p. 391.

[96] Ibid.

## Part Four: Structural Redundancy and Tradeoffs for NCO Command and Control

Information superiority accorded by NCO is not strictly confined to the collection of additional raw data but entails shared battle-space awareness among operating units that are derived from the efficient and reliable processing of information within a military organization. According to Mark Mandeles, this is best realized via informal and loosely coupled organizational structures that draw closely on insights from HRT.[97] Though there are benefits to centralized structures for planning and overseeing strategic operations, informal and loosely-coupled designs have advantages over formal, tightly-coupled hierarchical structures that include dispersed and decentralized decision authority, flexible and adaptable coordination and task responsibilities, and less rule bound procedures. These factors are expected to hold special promise for NCO, as senior decision-makers are less vulnerable to information manipulation of rigid procedures and reporting arrangements by sub-units, roles and tasks can evolve in response to problems and uncertainty, and decisions are the product of negotiation among component units that possess special expertise and experience with the issue at hand.[98] Similarly, there are incentive advantages of informal organizational designs that feature decentralized diffusion of tacit knowledge and division of authority among small groups, as well as the streamlined monitoring of professionalism and the decision process (not outcomes) by few levels of

[97] Mandeles (2005).

[98] James Desvaeaux, *Designing Bureaucracies: Institutional Capacity and Large-Scale Problem-Solving* (Stanford: Stanford University Press, 1995); James Q. Wilson, *Bureaucracy: What Government Agencies Do and Why They Do It* (new York: Basic Books, 1989). For application to the NCO context, see especially summary in Mandeles (2005), pp. 147-158,

hierarchy to coordinate action.[99] This is especially relevant for decisions taken in the face of uncertainty, ambiguity, imperfect information, and tight deadlines.

Yet, the utility of HRT structures is not universal. As noted by Mandeles, reliance on tight coupling for selective strategic network centric tasks is warranted with the more causal knowledge and focus obtained by a command authority. In short, the appropriateness of organizational structure rests on the balance of trade-offs among specific design criteria that turns on the meaning and significance of redundancy.

### *Redundancy vs. Centralization*

As discussed above, the appropriateness and efficacy of loosely coupled designs for NCO derive from understandings of the performance of HRO. The keys to efficient information gathering and processing in such organizations rest with redundancy and the informal transmission of tacit knowledge that facilitate closely synchronized coordination within otherwise hierarchical structures. Individual units are assigned overlapping authority and perform a variety of roles in informal networks that are self-regulated and adapt to the nature of a problem. Continuous training among problem-specific units lies at the heart of effective information gathering, transmission, and processing. High reliability is ensured by the informal interaction among multiple, independent, redundant units. This school considers the relationship between the number of redundant human and mechanical devices and the probability of failure as inversely proportional. The underlying logic derives from mathematic models that demonstrate

[99] Mandeles (2005), pp. 158-165.

that the product of failure rates among independently operated units drops to nearly zero with only a limited number of redundancy measures.[100] Similarly, the high reliability school contends that increased human redundancy decreases the likelihood of failure.[101] To support their argument, proponents look to peacetime operations aboard U.S. aircraft carriers, where Navy personnel are assigned different yet overlapping tasks to ensure that critical problems are identified and redressed.[102]

The beauty of redundant organizations for managing future NCO is at least threefold. First, constructive and competitive duplication, it is argued, can mitigate the monopoly power, inconsistency, and perverse consequences of meddling of a single commander.[103] Second, as argued by Landau and Bendor, redundant administration carries the advantage of increasing system reliability without demanding an increase in the reliability of organizational sub-units. As long as constituent elements are independent and parallel, redundancy can reduce the risks of system failure to significantly low levels.[104] Third, redundancy speaks to the prospects for addressing a primary concern with NCO command- system reliability—at the expense of secondary concerns, such as efficiency, that may be gained via competition. Given the compounded costs to NCO of blowback and the circulation of incomplete or poor information, there is a premium placed on developing failsafe command and control structures.[105]

[100] "Suppose an automobile had dual breaking (sic) circuits: each circuit can stop the car, and the circuits operate independently so that if one malfunctions it does not impair the other. If the probability of either one failing is 1/10, the probability of both failing simultaneously is $(1/10)^2$ or 1/100. Add a third independent circuit and the probability of the catastrophic failure of no brake at all drops to $(1/10)^3$ or 1/1000." See quote from Sagan (1993), p. 20.
[101] Sagan (1993), p. 20.
[102] Ibid.
[103] Niskanen, (1971), pp, 197-199.
[104] Landau (1969), pp. 352-353; and Bendor (1985).
[105] Bendor (1985), p. 54.

The potential panacea for information overload offered by redundancy has not been lost on NCO advocates. As asserted by James Freebersyser of DARPA's Advanced Technology Office and Joseph Macker of the Naval Research Laboratory, "the mission critical nature of shared information demands robustness, redundancy, and survivability."[106] Furthermore, the Program Executive Office for C4I within SPAWAR identified the need to increase technical redundancy as a future objective for NCW.[107] Similarly, Arthur Cebrowski maintained that both technical and human redundancy were critical to NCO.[108] Based on a recent assessment conducted by Commander Richard Gomez, it appears that the Navy has taken Cebrowski's advice and engineered redundancy into the network along with a rapid recovery capability.[109]

Notwithstanding the enthusiasm, the assumptions about high reliability organizations that lie at the heart of NCO are problematic. On the matter of technical redundancy, insights from "normal accident theory" suggest that redundancy can reduce the probability of failure, but only under certain conditions. Given assumptions that incidents cannot be averted altogether, organizations should be structured in a manner conducive to containing a problem. As a result, normal accident theory emphasizes high system visibility that can ease rapid response times.

[106] James Freebersyser and Joseph Macker, "Realizing the Network-Centric Warfare Vision: Network Technology Challenges and Guidelines" http://tang.itd.nrl.navy.mil/5522/pubs/pdf_papers/netcentric_milcom01.pdf#search=%22%E2%80%9CRealizing%20the%20Network-Centric%20Warfare%20Vision%3A%20Network%20Technology%20Challenges%20and%20Guidelines%E2%80%9D%22 (accessed 30 July 2006).

[107] Michael Brunskill, "PEO C4I Innovative Advances in C4ISR" http://www.afcea.org/events/pastevents/documents/CAPTMichaelBrunskill.ppt. (accessed 30 July 2006)

[108] Cebrowski, (2003), p. 20.

[109] Although not self-repairing, the rapid recovery capability allows for the disrupted communication centers to transfer their traffic should they become incapacitated; Richard Gomez, "Centralized Command – Decentralized Execution: Implications for Operating a Network Centric Environment" http://www.au.af.mil/au/awc/awcgate/awc/gomez2003.pdf#search=%22Centralized%20Command%20Decentralized%20Execution%3A%20Implications%20for%20Operating%20a%20Network%20Centric%20Environment%22 (accessed 30 July 2006)

However, adding more technological solutions only increases the complexity of the system that, in turn, reduces its visibility. Charles Perrow, for example, notes that during the Three Mile Island (TMI) accident, the excessive use of redundant devices raised so many red flags that it took nearly two hours for the computer to register the real cause of the problem.[110] Meanwhile, the engineers and operators operated under false pretenses and intensified the problem. Furthermore, Perrow comments that redundant devices offer no safety guarantees because future incidents can bypass such measures as well.[111] Accordingly, it is important to evaluate the tradeoffs between decreasing failure probabilities and increasing the complexity of the system. By containing redundancy and focusing on transparency, commanders will be able to minimize the complexity of the system while improving prospects for detecting system failure. But that will be a large and complex task and the history of technology does not provide much optimism. As we have previously noted in last year's report Managing Transformation into the Future: Network Operations and the US Navy, the Department of the Navy lists two tentative timelines for an operational capability for each technology supported function: initial and final. The main functions – ForceNet, Sea Shield, Sea Basing, and Sea Strike – will reach their final operating capabilities only by 2020 and only ForceNet will reach initial operating capability before 2015. As of 2005, the Navy had roughly 20 of 74 technologies at their initial operating capability and zero at the final operating capability. How will this transformation be managed as a coherent whole? According to Perrow each new technological innovation or fix carries within it a new and wholly unanticipated set of technological and organizational problems. This does not bode

[110] Perrow (1999), p. 28.
[111] Ibid., p. 4.

well for such an ambitious undertaking, and the issue of redundancy as the panacea for the maladies associated with normal accidents is at best a minor sub-theme.

In addition, there are several fundamental shortcomings with the standard treatment of redundancy. First, there are definitional problems that conflate the concept with competition, duplication and overlapping structures. As Bendor notes, "all competitive structures are redundant but the converse is not true, there are noncompetitive types of duplication."[112] Overlapping structures that strengthen redundancy via ambiguity, nonetheless violate Landau's assumption of independence and parallelism. As long as there is some possibility of interaction between components that risk of common-mode error, the value of redundancy can easily be lost. By the same token, duplication, which is premised on providing similar organizational services via identical systems, under different conditions can produce redundancy at the cost of either excess waste, stress, or shadow reserves; each with different tradeoffs for intra-organizational efficiency and incentives.[113] Duplication, in particular, can exacerbate coordination problems by generating excessively high transaction costs among sub-units and failing to address priority, as opposed to non-urgent and standard issues, especially should commander lack valuable private information. These can be especially problematic for NCO that place a premium on real-time information processing and combat effectiveness, synchronized activity, and the employment of identical or at least compatible standards among constituent elements.[114]

[112] Bendor (1985), p. 54.
[113] Rowan Miranda and Allan Lerner, "Bureaucracy, Organizational Redundancy, and the Privatization of Public services," *Public Administration Review* 55:2 (March/April 1995), pp. 193-200.
[114] Patrick Bolton and Joseph Farrell, "Decentralization, Duplication, and Delay," *The Journal of Political Economy* 98:4 (August 1990), pp. 803-826.

Second, constructive competition can take both intra- and extra-organizational forms with different consequences for command and control. On the one hand, there are designs that feature splitting sub-unit mandates and pitting them as rivals in the performance of specific tasks. This can general productive information flow as long as communication channels are open and accessible. However, the benefits for oversight degrade if the agents perform indistinguishable and duplicate, as opposed to clearly delineated complementary, tasks. This is because the former runs a greater risk of generating a propensity for "adverse reputational herding," as the redundancy sub-units will tend to play to the lowest common denominator of competition in task performance quality. The same design feature also tends to be corrupted by oversight by a "friendly" versus professional commander. [115] These organizational maladies literally fall out of a description of the organizational arrangements surrounding ForceNet development identified in last year's report and again identified in Appendix B.

On the other hand, ex-organizational competition runs higher risks of incurring problems of collusion among redundant actors, as well as of generating problems of "premature lock in" and the narrowing of outside actors with the selection of lead agencies and contractors. As demonstrated by Oliver Williamson, the advantages of external competition are greatest when the assets of concern as less specific; alternatively, the more specific the performance task the

[115] This insight comes from George A. Krause and James W. Douglas, "Are Two Heads Always Better than One? Redundancy, Competition, and Task Performance Quality in Public Bureaus," paper presented at the 15th Annual Association of Budgeting and Financial Management, Washington, DC, September 18-20, 2003; and Michael M. ting, "A Strategic Theory of Bureaucratic Redundancy," *American Journal of Political Science* 47:2 (April 2003), pp. 274-292. On the advantages of clearly delineated, complementary tasks, see especially J. T. Hage, "Organizational Innovation and Organizational Change," *Annual Review of Sociology* 25 (1999), pp. 597-622.

more desirable it is to centralize oversight and preserve complementary but monopolistic authority among implementing actors.[116]

Third, NAT suggests that human redundancy may actually increase the likelihood for accidents, absent effective monitoring mechanisms. In particular, the theory draws distinction between inanimate mechanical components and human forms of redundancy. This derives primarily from the distribution of authority within an organization. As Scott Sagan notes, "Unlike technical devices, humans are aware of one another and the addition of an extra guard, or pilot, or radar watcher can lead other to be less observant or responsible."[117] For example, if person A and B are assigned to complete the same task, person A may not take up the slack or do a thorough job because she/he thinks Person B will catch her/his mistakes, whereas Person B thinks the same about Person A. Neither Person A nor B will have incentive to diligently complete the assigned task with the conflation of decisional authority. Unless properly supervised, duplication under these conditions may actually decrease system reliability by generating incentives for social shirking. Similarly, redundancy can backfire by encouraging parallel constituent agents to be either over-zealous or risky in the performance of tasks. This tendency of over-compensatory behavior in the face of safety and reliability improvements has been heavily studied, and is suggestive of more reckless task performance of NCO conducted by agents with blind faith in the vigilance of redundant peer units.[118]

[116] Miranda and Lerner (1995); and Oliver Williamson, *Markets and Hierarchies: Analysis and anti-trust Implications* (New York: Free Press, 1975).

[117] Scott Sagan, "Learning from *Normal Accidents*" *Organization and Environment* 17, no.1 (2004), 15 -16.

[118] Scott Sagan, "The Problem of Redundancy Problem: Why More Nuclear Security forces May Produce Less Nuclear Security," *Risk Analysis* 24:4 (2004), pp. 935-945.

## Part Five: Prospective Amendments to NAT and Future NCO Administration

As discerned from the discussion above, there is no single, comprehensive, optimal organizational design for NCO command and control. The all or nothing adoption of HRT or NAT assumptions is problematic, as there are tradeoffs of efficiency and reliability that are more versus less appropriate to the performance of discrete NCO, at the strategic, operational, and tactical levels. There are advantages and disadvantages to each on the redundancy issue alone. In contrast to the findings of HRT, for example, NAT offers several insights for containing information overload that restrict duplication. In his analysis of the Three Mile Island (TMI) accident, Perrow noted that the excessive number of red flags raised by the safety devices delayed the computer by nearly two hours, which left the engineers and operators to work under false pretenses.[119] This problem was exacerbated by the lack of direct measure devices at TMI led the workers to base their decisions off readings that did not consider the real issues.[120] To redress this problem, he warns against overzealous data collection, and contends that incoming information should be limited to specific issue areas of observation. In this regard, designating complementary, as opposed to duplicate sub-unit tasks, should assist with reducing system complexity and enabling faster response times.

The debate also suggests prospective designs to mitigating problems of operating in a false reality. Perrow draws on examples from the missile defense system at NORAD, where he

[119] Perrow (1999), p. 28.
[120] Ibid., pp. 24-27.

found several instances of 'the big board' projecting false images.[121] Here he notes that the missile commanders relied on the corroboration of these images with two other independent, direct measure sources before reacting to the readings.[122] Given the proposed reliance of NCO on information superiority, one lesson from NORAD might be to implement multiple independent direct measuring systems so as to prevent acting upon a fictitious set of assumptions. This measure also may help to defend against network sabotage by enemy forces, which is central to information warfare.

Similarly, "benchmarking" may offer a useful technique for combining the benefits from both HRT and NAT to enhance reliable and effective organizational information processing. In order to cultivate the benefits of extra-organizational competition and parallel redundancy, while minimizing dysfunctional duplication and maintaining command and control over real-time, priority tasks, commanders can resort to specifying centralized yardsticks, agendas, and directives at the same time that they delegate multiple agents to implement tasks. This form of "controlled competition" via benchmarking priorities and measurement criteria may offer a design to combine the benefits of centralization and redundancy, especially involving the performance of non-specific and integrated tasks.[123]

With respect to human redundancy, normal accident theory suggests the importance of clearly delineating authority among sub-units. While overlapping authority generates incentives for shirking, the delegation of separate but complementary responsibility should ensure diligent

[121] Ibid., pp. 284-288.
[122] Ibid.
[123] Miranda and Lerner (1995).

performance as well as ease oversight. The former, for example, vests sub-units with independent, discrete authority that carries specified costs and benefits of action. Moreover, as each authority becomes integrated (but independent) with another, commanders can create incentives for self-monitoring among subordinates and affected third parties. Unlike with technological measures where automatic integration may produce cascading problems, the separation of responsibility among human agents can ease the burden of direct oversight, thus allowing commanders to concentrate scarce time and resources on analyzing specific data.

In addition to the above administrative conditions, normal accidents theory stresses the importance of paying heed to basic principles of systems engineering. Accordingly, structuring the command organization and information processing system requires planning for an appropriate utilization rate in NCO. Typically, in industry, engineers only plan for a maximum utilization of between 80% and 85% that allows for relatively smooth operations regardless of varying process parameters. If NCO are designed with this same standard, then spikes in amount of incoming information should not push the command element into a state of information overload or false reality. This suggests that in order to achieve the prescribed utilization, a service should determine the following rates:

***Current Average*** Information Processing Rate (□)

In order to determine this rate for the system, one must breakdown the system into its subunits and uncover individual average processing rates. The overall average information processing rate for the system will be equal to slowest subunit's average processing rate. If the overall average system processing rate exceeds this, then that subunit will encounter information overload or operate in a false reality that would adversely effect the commander's final decision.

### ***Anticipated Average*** Information Arrival Rate (□)

This requires finding the highest single information influx rate and examining the circumstances that necessitated it. The rate generated by a large force engaged in closely coordinated and intense combat should provide the most demanding case. Otherwise, the highest single information arrival rate should be scaled to reflect the conditions of the above situation. These rates determine the utilization rate. If it is higher than 85%, then a military service may need to increase the processing capacity of the slowest subunit (bottleneck). Although the bottleneck may change with each iteration, this process should be continued until the following condition is satisfied.

$$\frac{\text{Anticipated Average Information Arrival Rate (□)}}{\text{Slowest Individual Average Information Processing Rate (□)}} < = 0.85$$

## Appendix A: Historical Perspectives on Transformation Successes and Failures

*Lessons From Historical Cases of Success*

The 2003 findings from our study of historical cases of successful military transformation (b)(5) – the adoption of carrier aviation in the U.S. Navy, the development of ballistic missiles during the Eisenhower Administration, and German armor development in the inter-war period -- suggest that there is room for cautious optimism regarding the prospects for military innovation.[124] Organizational barriers are neither intrinsic nor insurmountable. What is required, however, is perseverance in crafting a transformation strategy that blends continuity with change. The commitment to dramatic military change must be lodged, both institutionally and normatively, within each military service. As all three historical cases of success demonstrate, radical change can take place amidst conservative organizational leadership and cultures, provided that it is bred and proven from within the existing set of institutions. By speaking to a service's core competency, policy entrepreneurs and champions of change can use prevailing institutional constraints to their advantage for inducing military organizations to explore novel concepts and procedures. To do so, however, requires developing a strategy for managing transformation that adheres to at least six distinguishing guidelines.

***Manage transformation from within the services.*** Avoid creating an extra- service, civilian executive committee for transformation, charged with overseeing change across the

(b)(5)

services.[125] Outsiders are traditionally provided only limited access to service structures and resources that effectively ensures the burying of transformation ideas and the cannibalizing of new agendas. Alternatively, integrating the agency of change within a service provides incentives for change as well as a vehicle for monitoring developments within a service. In the U.S. carrier case, the decision to avoid hiving-off the Bureau of Aeronautics (BurAer) from the Navy, either by appending it to the Air Force or by orphaning it as a separate agency, gave naval personnel a stake in pursuing the carriers. Similarly, innovation was spurred in both the American missile and German armor cases by the creation of missile-specific development units within each service, as well as by the fluid and direct interaction between the Weapons Office and Branch Inspectorates within the German Army, respectively.

***Assure that champions of innovation are rewarded via traditional service lines of promotion and career paths.*** Rather than establishing new posts to reward and empower proponents of innovation, this study confirms the argument that the incentive for continuous exploration rests critically upon assuring access to mainstream promotion boards and officer assignments. As all three cases demonstrated, transformation supporters excelled when respective risk-taking efforts presented opportunities for them to rise to senior leadership positions within their service. In the carrier case, the combination of bonus payments for hazardous air duty and the assignment of a rear admiral billet ensured that promotion to the newly established Commander, Aircraft Squadrons, Battle Fleet would unambiguously further an officer's career within the U.S. Navy. Similarly, successful careers in the Weapons Office paved the way for promotions to commander positions in the respective Branch Inspectorates of the

[125] *Washington Times*, 24 April 2001.

German military. In some cases this also led to coveted line commander assignments. What is critical is that entrepreneurs were reassured that their exploits would not be held against them within their own service, and that their success would bring them closer, both professionally and institutionally, to their commanders. Thus, tying success to traditional promotional positions can codify an enduring incentive for innovation in emerging warfare areas within a service.

***Avoid ad hoc organizational mechanisms.*** Effecting a military transformation also entails that informal bodies that are created to promote innovation within a service reinforce formal mechanisms of reporting and reward. Critical for encouraging change in all three historical cases were clearly delineated lines of responsibility within each service. While champions of innovation tended to create and exploit informal channels to facilitate internal coordination and managerial oversight of innovation, they did so in manners that complemented the formal chain of command. In the carrier case, for example, a back-channel was created between the BurAer, the Fleet, and the Naval War College that expedited the generation and dissemination of realistic scenarios of future naval warfare. This enabled all three to work off the same page in terms of structuring and analyzing the implications of experimental models and fleet exercises. In addition, an informal link was established between the head of BurAer and the Commander, Aircraft Squadrons, Battle Fleet that allowed both to focus on the tasks of monitoring respective sub-components without spawning inefficient bureaucratic or personal rivalry. This effort at coordinating was reinforced by the informal practice of circulating personnel across the bureau-fleet divide, and by rotating naval aviators to positions outside of the service in academia and industry. Similarly, the services established informal liaisons between respective missile development units that augmented the exchange of information. The reciprocal sharing of technical insights facilitated learning between the Army and Air Force design teams, enabling each to redress problems encountered with the development of turbopumps for the Jupiter and Thor IRBMs, respectively. In addition, informal exchanges between the two services allowed Air Force missile designers to capitalize on the Army's successful development of ablation techniques for nose-cone re-entry of ballistic missiles.

***Embrace the evidentiary as well as the dominant strategic culture within each service.*** What emerges from these earlier cases of transformation is that the prevailing and conservative organizational cultures, whether it be the "Big Gun Club" in the U.S. Navy or the "pilot culture" of the U.S. Air Force, are neither static nor uni-dimensional. In each case, the dominant normative predisposition of the service was embraced by successful entrepreneurs, not tackled head on or bludgeoned into accepting transformation. The prevailing service cultures proved to be significantly malleable and were adroitly converted into assets for lowering the agency costs of managing change. This was achieved by initially "selling" innovations as consistent with the dominant strategic beliefs within each service, and then by exploiting respective "evidentiary standards" to communicate new information that confirmed novel ideas but not traditional expectations. Tapping into both accepted strategic missions and rules of evidence gave service entrepreneurs persuasion power; they acted not only as critics but offered socially salient solutions to traditional problems that served as new focal points for preparing for and waging war within the services.

All three cases stand out in this regard. The carriers were initially proposed as an instrument for fulfilling the main mission of "fighting across the Pacific," and as an auxiliary to the dominant battleship in the U.S. Navy. Support from the orthodox "Gun Club" was co-opted ultimately by demonstrating the potential effectiveness of the carriers in common terms. In particular, the Navy's traditional acceptance of technical evidence, culled from extensive war gaming and fleet exercises, was used to demonstrate gaps between traditional expectations and the potential payoffs of adopting the carriers. This not only provided a standard for updating information on the potential effectiveness of the carriers but reduced the need for intrusive monitoring among decentralized sub-units within the Navy. Similarly, the proponents of innovation effectively plugged into the shared belief in the value of mobility and maneuver within the German Army. Seeckt and other champions also embraced the long-standing German Army preference for decentralization, technical education, critical assessment of open-ended experimentation, and high error tolerance to manage the process of transformation. Alternatively, in the missile case, the U.S. Air Force's rigid adherence to manned aircraft and resistance to disconfirming evidence was partially circumvented by pitching the case for missiles in terms of the service's sensitivity for maintaining its independence. This was done by presenting evidence of the success achieved by other services at developing unmanned combat vehicles, and by underscoring the risks that this posed for inter-service poaching of the Air Force's prized mission of "strategic bombing."

***Intensify competition, either at the sub-unit or service levels, with greater toleration for honest failures and short-term mission redundancy.*** The historical cases examined in this study revealed that more not less competition, both between the services and among sub-units within a service, augurs well for transformation, especially in those areas involving the development of a fungible technology. Such competition can mitigate the inefficiencies fostered by information asymmetries within a hierarchical military organization by providing indirect, alternative sources of information for entrepreneurs. It also can create incentives for exploring new capabilities and solving old technical problems. In the carrier case, inter-service competition with the U.S. Army and Marine Corps yielded critical information that the proponents of the carriers used to raise the bar for the development of naval dive-bombers. Alternatively, the missile case was characterized by the horizontal, intra-service shielding of design teams, as well as by inter-service competition among the teams. Missile entrepreneurs effectively reduced agency costs within each service by fostering competition for "market share" in the development of this modern weapon. As mentioned above, design teams were able to learn from each other in this process, exploiting advances in ballistic missile technology achieved by one to advance the respective development programs of the others.

***Rely on extra-military institutions to promote transparency, not intrusive oversight.*** Outside forces can serve as enablers of internal military transformation. External actors, such as the U.S. Congress and industry, that maintain independent stakes in promoting successful innovation, can provide reliable, low cost alternative sources of information for managing change from above. While abstaining from the policy game, the U.S. Congress played an indirect role in facilitating naval transformation by institutionalizing formal promotional incentives for carrier innovation, and ensuring that naval aviators would not be orphaned either within the Navy or armed forces in general. Without intervening directly or mandating the outcome of naval debates, Congress indirectly smoothed the path for change by rooting out corrupt practices and fostering an even playing field that provided carrier entrepreneurs with opportunities to make their case within the Navy. President Eisenhower assumed an analogous role in the missile case. While he was uniquely capable of defending programmatic characteristics, he was careful not to interfere intrusively in service debates except to facilitate information sharing between service design teams.

Industry too can be enlisted to reduce agency costs of managing organization change. Rather than providing a managerial model to emulate, the private sector served as an independent source of information regarding the possible application of new technologies. The practices of sharing contractors and promoting competitive contracting for missile sub-systems stimulated incentives to innovate and exchange information. This, in turn, mitigated information asymmetries between commanders and design teams within each service. In the carrier case, the reciprocal flow of information between private contractors and Navy fostered entrepreneurship on both sides. Close ties with the commercial aviation industry allowed the champions of carrier aviation to glean detailed information regarding possible applications of new engine technologies that were not otherwise provided from within the naval hierarchy. At the same time, once the BurAer decided upon an engine for procurement, it was able to use its contracting authority to dampen the monopolistic tendencies within industry and to cultivate commercial support for developing a novel prototype technology that was otherwise slated to languish.

*Lessons From Historical Cases of Failure*

The cases synopsized above demonstrate how proper principle-agent relationships can determine balances between organizational strategies of exploration and exploitation promoting successful military transformation. (b)(5)

(b)(5)

Failure, from this perspective, pertains to the discrepancy between the potential operational value presented by accepted technological innovations and the level by which this potential is realized and institutionalized within a military organization. Accordingly, failure is distinct from the inability to produce technological innovations or to achieve victory on the battlefield. Rather, it is a managerial issue that reflects an organization's deficiency at creating lasting structures and procedures that are appropriate for fully exploiting new technologies and task environments. In the case studies of failure – aircraft carrier development in the British Navy and armored doctrine development in the British Army during the inter-war period, and mal-adaptation of U.S. counter-insurgency strategy in Vietnam -- these obstacles were not successfully overcome.

Organizational innovation is neither intrinsic nor impossible. What is required, however, is perseverance in crafting a transformation strategy that blends continuity with change. The commitment to dramatic military change must be lodged, both institutionally and normatively, within each military service. As all three historical cases of failure demonstrate, radical change can be stymied even when service entrepreneurs acknowledge the potential pay-offs of new technologies and settle on new ideas of war. Innovative forms and methods can be resisted if they are not bred or proven from within the existing set of institutions. By failing to speak to and organize around a service's core competency, policy entrepreneurs and the champions of change risk compounding the difficulties of inducing sub-units to explore novel concepts and procedures. Avoidance of these undesirable outcomes and success at turning institutional

(b)(5)

constraints to the advantage of promoting organizational change require developing a strategy for managing transformation that adheres to at least six distinguishing guidelines that were initially gleaned from the previous study of classic cases of success.

The obvious failure to follow these guidelines for successful transformation comprise the heart of the three extensive case studies in the report. The guidelines for success and a brief summary of failure, drawn from one or more of the cases, follows.

***Manage transformation from within a service by establishing clear lines of authority and responsibility***. Integrate novel offices for supervising change within a service. This provides incentives for change as well as a vehicle for monitoring developments within that service. As evidenced in all three case studies, the creation of an extra-service agency or executive committee charged with directly overseeing change within a service created both administrative confusion and disincentives for transformation. Outsiders are traditionally provided only limited access to service structures and resources, as well as tend to provoke professional resistance, that together lead to the burying or dilution of transformation ideas and the cannibalizing of new agendas. In the British carrier case, the imposition of "dual control" between the Royal Navy and Royal Air Force over naval aviation cost Britain its early lead in carrier development by discouraging exploration of an independent mission and hampering requisite training, assessment and procurement of the naval air wing. It was not until 1939, when the Fleet Air Arm was firmly placed back under to the exclusive operational and administrative jurisdiction of the British Navy, that novel spotting, gunnery, and mass- air offensive operations were institutionalized for carrier aviation. Although by that time the British Navy was presented with the difficult responsibility of coping simultaneously with fiscal stringency, rapid technological innovation, and the gathering winds of war, it nonetheless succeeded at introducing novel designs for armored flight decks.

***Assure that champions of innovation are rewarded via mainstream service lines of promotion and career paths***. Rather than establishing new posts to reward and empower proponents of innovation, this study affirms the earlier finding that the incentive for continuous exploration rests critically upon assuring access to mainstream promotion boards and officer assignments. All three cases demonstrated that support for transformation waned when respective risk-taking efforts were neither directly rewarded nor closely integrated with core promotional pathways to senior leadership positions within the respective service. In the British armor case, the institutional uncertainty about the status of the tank discouraged officers from staking their careers on the Tank Corps. Even with the formation of the Royal Tank Corps as a separate branch of the Army, senior officers were transferred from other branches (with no experience in armor) that effectively precluded advancement for the early champions of the tank. The incentives for innovation did not increase over time, as promotion both within the branch and up through the service was determined to a great extent by seniority, regimental peculiarities, and versatility at serving at home and within the imperial ranks rather than by specialization. The disincentives were exacerbated by the creation of the Royal Armored Corps, consisting of both mechanized and armored units, that gave a leg up to officers with extensive cavalry experience, and by the institutional constraints on conducting well-coordinated, combined training exercises. Although several tank enthusiasts were promoted to senior Army ranks during the period, their rise occurred almost in spite of rather than because of their affiliation or performance working with tanks.

***Avoid creating isolated, ad hoc organizational mechanisms.*** Effecting military transformation also entails that the *ad hoc* bodies that are created to promote innovation within a service reinforce formal mechanisms of reporting and reward. Confused lines of authority constituted significant impediments to sustaining change in all three historical cases. While champions of innovation tended to establish and exploit informal channels to facilitate internal coordination and managerial oversight of innovation, they did so in manners that confounded the formal chain of command. Although President Kennedy created the position of Special Assistant for Counter-Insurgency and Special Activities (SACSA) to increase the profile and legitimacy of the Army's Special Forces, the position both lacked a constituency and circumvented the Special Forces Command within the service. Consequently (and irrespective of personal differences in counter-insurgency expertise and rapport with the president), successive advisors were consistently treated as "outsiders" and encountered problems working within the service.

***Embrace the strategic and managerial norms of the respective service***. What emerges from these earlier cases of transformation failure is that the respective services were neither excessively conservative nor hardwired to resist change. Although the British Army did not successfully exploit the tank's operational potential, it was not significantly hampered by an overly conservative military leadership that failed to envision the utility of army mechanization. Similarly, the British Navy embraced the concept of "flying squadrons" and amalgamated officer training, as well as devoted attention to conducting combined naval exercises, simulations, and devising a common standard for evaluating new missions and performance of naval aviation. Moreover, the U.S. Army proved adept at altering its force structure before committing troops to Vietnam by institutionalizing a new airmobile division. Instead, what distinguished the managerial failure in each case was the inability by service entrepreneurs to tap into established normative traditions in support of change. Although the prevailing service culture proved to be significantly malleable, in each case the champions of change failed to convert it into an asset for lowering the agency costs of managing change. Lacking empathy as well as a constituency, these novel concepts tended to fall on deaf ears within the respective service. The entrepreneurs failed to enlist the strategic mission or to present "new solutions" to old problems. They failed to exploit respective "evidentiary standards" to communicate new information or to "legitimate" novel ideas within traditional managerial norms. They chose instead to bludgeon the service into transformation. As a consequence, these entrepreneurs and their "radical" ideas were discredited and lost influence within the mainstream service.

***Intensify competition, either at the sub-unit or service levels, with greater toleration for honest failures and short-term mission redundancy***. The historical cases examined in this study affirmed that more not less competition, both between the services and among service sub-units, augurs well for transformation, especially in those areas involving the development of a fungible technology. The absence of such competition can aggravate inefficiencies fostered by information asymmetries within a hierarchical military organization by depriving entrepreneurs of indirect, alternative sources of information. Organizational isolation can discourage the exploration of new capabilities and the solving of old technical problems. In the counter-insurgency case, the early effectiveness of the Marines' Combined Action Program highlighted the prospects for pacification as well as provided a potential benchmark for assessing the Army's performance and subsequent initiatives at "village security" that was woefully ignored. Moreover, sub-unit competition among Special Forces units that were under Army and CIA direction offered insights into the possible success of counter-insurgency. However, once the Army was put in charge of planning, evaluating and implementation all counter-insurgency operations, Special Forces commanders lost an important source of alternative information for assessing the prospects for unconventional, defensive operations.

***Rely on extra-military institutions to promote transparency, not intrusive oversight***. Outside forces can serve as enablers of internal military transformation. External actors, such as the legislature and industry, that maintain independent stakes in promoting successful innovation, can provide reliable, low cost alternative sources of information for managing change from above. Conversely, external actors can compound the managerial challenge by providing cover for recalcitrant agents. President Kennedy' enthusiastic support for counter-insurgency alienated traditionalists within the Army. His penchant for micromanaging the issue also confounded the task, as he was driven to appoint advisors who were both too iconoclastic and mainstream to successfully "sell" counter-insurgency within the service. Congress also muddled the process of institutionalizing counter-insurgency. By formally abstaining from the policy game, the U.S. Congress did not provide a forum for entrepreneurs to make their case. At the same time, the risk-averse Congress generally played an indirect role in complicating oversight of counter-insurgency operations within the U.S. Army, as powerful congressional committees offered venues for conservative Army leaders to question new directives and budgetary appropriations.

## Appendix B: NCO Command Structure

The Navy's major NCO commands are rife with the problems of redundancy. In particular, the service has created multiple organs with overlapping authority that have confused oversight and generated pressures for shirking. NETWARCOM, for example, is the Navy's Central Operational Authority for Network and Information Operations. It was established on July 11, 2002. It is a 3-star department currently on its third commander in less than 4 years. Its headquarters and operations are in an enormous trailer park in Naval Amphibious Base Little Creek in Norfolk, Va. The only permanent structure is the command building. It does not convey the sense of permanence. NETWARCOM reports to commander, U.S. Fleet Forces Command. It is considered a 'Type Commander.' It provides long range planning of IT emergence - especially in Information Assurance and Information Operations. It covers all Navy networks and establishes policies and standards for them. It initially contained 45 billets – 8 enlisted and 37 officers + 15 civil service employees, but has grown much larger since.

NETWARCOM has a leading role in developing and creating FORCEnet. It also serves as the sponsor for the new restricted line community of officers known as information professionals. At various times the research team was informed that the information professional designation was a place to put the "radio operators from the old Navy" or a place for female officers. The community started out with about 330 officers, but the total has grown as the result of semi-annual officer selection boards. The Navy formally introduced a mentoring program for IP officers in August 2002.

The subordinate commands listed on the NETWARCOM website are:

SPAWAR - Space and Naval Warfare Systems Command (in error?)
NNSOC - Naval Network and Space Operations Command
CNSG - Commander Naval Security Group
FIWC - Fleet Information Warfare Center
NCTF-CND - Navy Component Task Force for Computer Network Defense
DCMS - Director, Communications Security Material System

It is instructive to note that SPAWAR, a much larger, older, and richer organization was initially a competitor to NETWARCOM, then after criticism from the Congress and the GAO, was made, briefly, a subordinate command of NETWARCOM, then almost immediately reverted to an extra duty assignment organization for NETWARCOM, preserving its independence. While NETWARCOM still lists SPAWAR as a subordinate command on its website, SPAWAR makes virtually no mention of NETWARCOM on its website. SPAWAR is discussed later in this section.

NNSOC – Naval Network and Space Operations Command

Formed from the merger of the Naval Space Command and Naval Network Operations Command, in July of 2002, NNSOC is responsible for managing world-wide communications to move towards increased NETWARCOM and Sea Power 21 capabilities, supporting the NETWARCOM communications in moving to IT-21, and finding system vulnerabilities in hostile spaces. NNSOC is a major hub of communications for all sectors of the Navy and serves as a new space for the innovation of interconnectivity for NCW. This office is still fairly new and is working on establishing itself. It does, however, already boast some of the highest speed and quantity of information transmitted, nearly doubling previous transmission capabilities for Operation Iraqi Freedom. The commanding officer is Rear Adm. John P. Cryer, and it is in Dahlgren, VA.

(b)(5)

FIWC – Fleet Information Warfare Center

The FIWC is the Navy's Center of Excellence for Information Operations. There are numerous roles set aside for this department. The first is to function as the Navy's training center for Navy IO operations. The second is to support the fleet's attempts to incorporate IO operations. The third is to advocate for new IO programs and the necessary support functions that accompany them. The fourth is to act as the Navy's primary agent for the formulation of IO doctrine and tactics, techniques, and procedures. Their fifth, and final, mission is to act as NETWARCOM's principle agent for identifying future technologies and capabilities to support future warfare and non-kinetic operations in the support of Sea Trial. FIWC was established in 1995 and is headquartered in Norfolk, Virginia. The FIWC is commanded by an 0-6. FIWC also provides computer and network vulnerability assessments for different Navy Commands. It also monitors network traffic in and out of the Navy's networks and notifies system administrators when their computers are compromised.

NCTF-CND -- Navy Component Task Force for Computer Network Defense

The mission of the Navy Component Task Force is to coordinate the defense of Navy computer networks and systems. The component directly supports the Navy's commitment to Presidential Decision Directive (PDD-63), Critical Infrastructure Protection, and Joint Vision 2010 Full Spectrum Dominance, which includes the capability to collect, process, and disseminate a secure uninterrupted flow of information. This mission includes the coordination of Navy defensive actions with non-Navy government agencies and appropriate private organizations. They are designed to run continuous IA vulnerability alerts.

DCMS – Director, Communications Security Material System

Located in Washington D.C., this department is designed to handle and support the Navy's "COMSEC material throughout the Department of the Navy, Marine Corps, Coast Guard, Military Sealift Command and National COMSEC community."[127] Additionally, the department is charged with support and guidance of the Navy's Information Assurance programs as the Navy's IA Publications Manager.[128]

[127] Director, Communications Security Material System. Department of Navy. 02 Apr. 2004 <http://www.netwarcom.navy.mil/dcms/mission.htm>.
[128] Ibid.

The following is a listing of other players in the information warfare, information security orbit relevant to the Navy's network centric operations plan. The list excludes DISA.

### SPAWAR - SPACE AND NAVAL WARFARE SYSTEMS COMMAND

SPAWAR's basic mission is to help the Navy communicate and share information. Its core capability is in C4ISR systems acquisition and life cycle management. It works in conjunction with and as an extra duty assignment NETWARCOM to provide NCW capabilities to Navy Warfighters. It is the chief architect and assessor for FORCEnet. It is a 3 star billet. SPAWAR is based in San Diego, but has offices in New Orleans, Norfolk (Space and Naval Warfare Systems Center), and Charleston each of which is focused on a specific task. SPAWAR started as the Naval Electronic Systems Command (NAVELEX) in 1966. In 1985, it was renamed to SPAWAR and given Echelon II status under the CNO. During this transition, it also took on the primary responsibility as the Navy's primary C4ISR architect. SPAWAR now contains a workforce of over 7500 employees dedicated to C4ISR, IT and Space systems for the Navy and $5.4 billion in TOA. It dwarfs NETWARCOM, and since it does not mention NETWARCOM on it website while giving much ink to FORCEnet on which NETWARCOM is supposed to be the lead agency, it begs the question of NETWARCOM's role and permanence.

SPAWAR Programs include the following:
Space Field Activity Chantilly
Naval-NRO Coordination Group
SPAWAR Reserve Program
Navy Communications Satellite Program Office (PMW146)
Operational Effects Program (PMW150)

Tactical Command Support Systems (PMW151)

Navigations Systems (PMW156)

Naval Command and Control Systems (PMW157)

Advanced Tactical Data Link Systems (PMW159)

Information Systems Security (PMW161)

Navy Marine Corps Intranet (PMW164)

Naval Afloat Networks (PMW165)

Naval Messaging Systems (PMW166)

Submarine Communications (PMW173)

Navy Satellite Communications (PMW176)

Advanced Automatic Tactical Communications (PMW179)

Naval Electronic Combat Surveillance Systems (PMW189)