VOLUME I

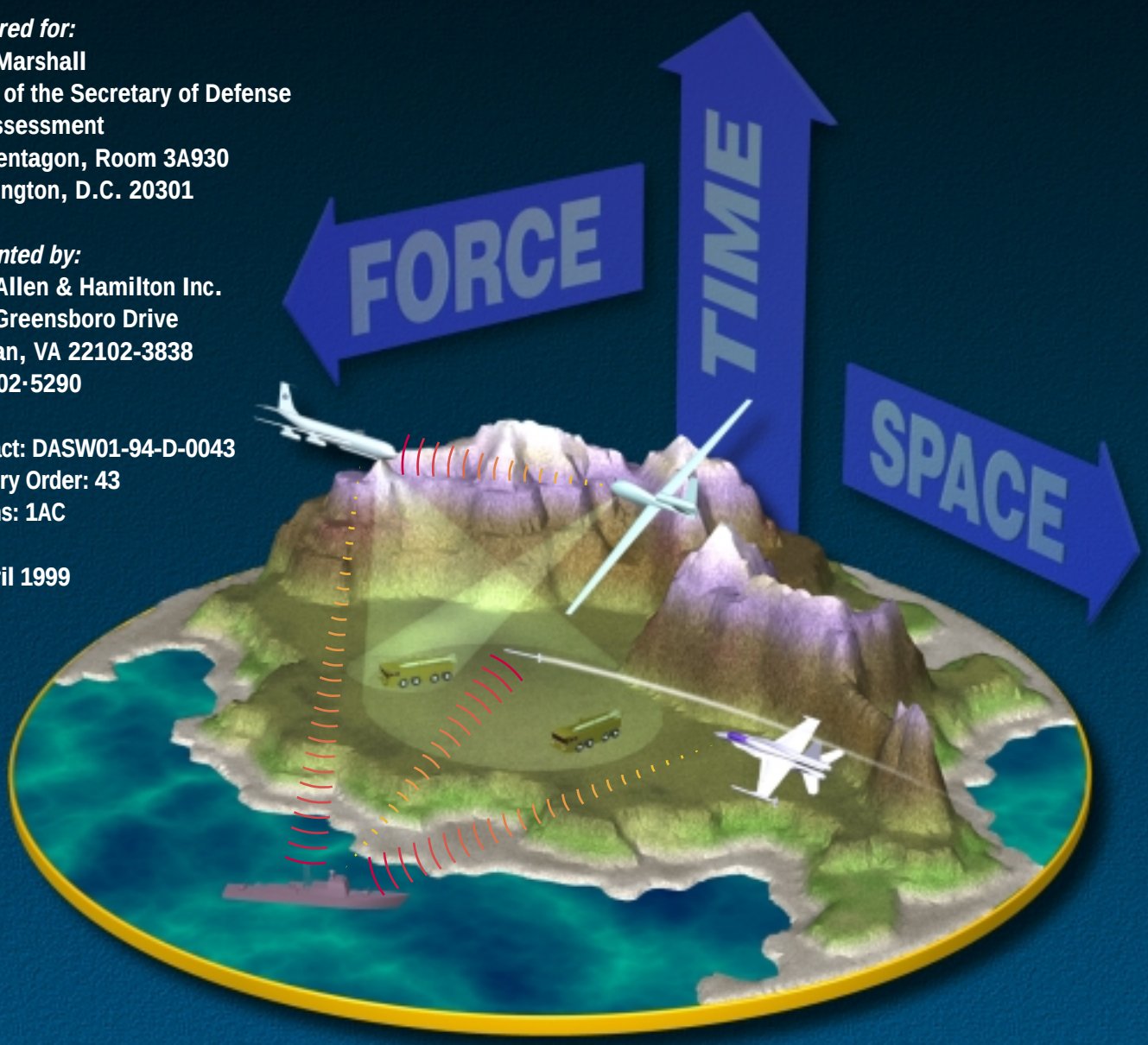
Measuring the Effects of Network-Centric Warfare

Prepared for:
A.W. Marshall
Office of the Secretary of Defense
Net Assessment
The Pentagon, Room 3A930
Washington, D.C. 20301

Presented by:
Booz·Allen & Hamilton Inc.
8283 Greensboro Drive
McLean, VA 22102-3838
703·902·5290

Contract: DASW01-94-D-0043
Delivery Order: 43
Options: 1AC

28 April 1999



BOOZ·ALLEN & HAMILTON

The views, opinions, and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of Defense position, policy, or decision.

EXECUTIVE SUMMARY

Background

The goal of this paper is to present a series of quantifiable metrics that can be employed to measure Network-Centric Warfare. These metrics are intended for use in Navy and Joint Experimentation to capture the data which will refine the emerging concepts of operation that will define future Navy and Joint doctrine. The metrics within this paper have been placed in an operational example to put them in context, but the scenario and its results are for illustrative purposes only. Based on the development of these metrics, it appears to the authors that there are two phases in the implementation of Network-Centric Warfare. The first phase will see the Navy, and potentially the other services, build a comprehensive linked network to optimize their legacy force structure. The second phase will see a new force structure emerge that will optimize this new concepts of warfare.

All new concepts of warfare must be measured in the context of the unchanging elements of war: force, space, and time. These dimensions represent the core elements that have impacted human conflict over the course of known history. The great captains of history were those unique individuals who played these elements together into a harmonious whole. Within this framework, the physical elements -- that is, the movement of men and material, or force, across physical space and time -- have always been emphasized. However, the domain of force is not the only area worth measuring, although it is the easiest. A true Revolution in Military Affairs involves more than technology; it also includes dramatic changes in organizational structures and processes. In fact, cognitive (reason) and behavioral (belief) aspects promise to play a greater role in the Information-based RMA than technology alone, and may have a greater influence on overall battle outcomes (Napoleon believed that "the moral is to the physical as 3 is to 1"). The domain of reason is the realm of human understanding, cognition, and decision-making. The belief domain is the realm of human and organizational behavior and includes individual morale, leadership, group cohesion, and the willingness to risk life and limb.

Introduction

Network-Centric Warfare implies that war should be viewed as a complex adaptive system. It is complex in that it is composed of the non-linear interaction of many variables. It is adaptive in the sense that the agents use feedback mechanisms to adapt to and exploit their environment. It is a system composed of hundreds of nested systems and sub-systems that strive to operate in unison. The key tenets of Network-Centric Warfare are the concepts of "Thin Shooter", "Speed of Command," and "Self-synchronization." These tenets are based on a simple hypothesis: "The principal utility of information superiority is time – the immense advantage of being able to develop very [1] Network-Centric Warfare is a shift in focus from the physical domain trumpeted by classic attrition theory and the spatial dimension expounded by classical maneuver theory to the temporal dimension. Moreover, the tenets of Network-

[1] VADM Arthur K. Cebrowski, "Sea Change," *Surface Warfare*, November/December 1997, p. 4

Centric Warfare (i.e., speed of command and self-synchronization) suggest a shift away from the physical domain to the reason and belief domains of war. The shift from the platform to the network is also a shift from a closed to an open system in warfare where actors are no longer independent but part of a "continuously adapting ecosystem."[2].

Key Attributes and Vulnerabilities of NCW

Throughout the paper, a number of different attributes of NCW repeatedly surfaced during the analysis. The first key attribute of NCW is its ability to allow friendly forces to operate in a dispersed manner without sacrificing operational capability. A dispersed force complicates the enemy's targeting problems, which will only become more critical in the future as enemies continue to advance their sensor-to-shooter systems hence making it more robust. The second key attribute is the responsiveness offered by improved C4 and connectivity. Gaining the temporal advantage (turning information into effects faster) provides a commander with a much wider range of options than a commander forced to react. When the timeliness is combined with a networked force, the commander is then capable of orchestrating truly simultaneous operations. Finally, a Common Operating Picture will allow each unit on the network to respond to each of the threats reducing the overall potential risk, provided it depicts the information relevant to that particular threat. The response could come in the form of a self-synchronized force responding to each threat based on the commander's intent or reduce the incidences of friendly fire.

On the other hand, there was one particular vulnerability of NCW that also cuts across all facets of military operations. The vulnerability concerns the requirement to maintain the timely flow of information and communications through the networks. If the information is not available to the key commanders or units at a critical time, then the lighter, dispersed forces will be in danger of being overpowered by traditionally deployed heavier forces – i.e., a thin shooter is implicitly more vulnerable when isolated than a heavy shooter. Additionally, there is a potential limitation of the Navy's ability to maximize the benefits of NCW in that the service must train and develop commanders and sailors to operate in this information-rich environment. This training must include improving the increasingly important man-machine interface to allow for more rapid decision-making.

Modeling NCW

With its emphasis on time and effects, it is unlikely that improvements promised by Network-Centric Warfare can be captured by analysis and modeling and simulation focused on force and attrition alone. New emphasis on the domains of reason and belief are required. Thus, to properly capture the impact of Network-Centric Warfare, a modeling and simulation paradigm shift from platform-based to effects-based must occur. Moreover, the modeling paradigm needs to shift from focusing on discrete physical events to capturing larger system effects. In such a shift, traditional metrics of effectiveness, efficiency, and robustness are still applicable, although the measures of performance that support these higher level metrics will change. Moreover, the context in which the modeling and simulation occurs needs to be enlarged from measuring purely

[2] VADM Arthur K. Cebrowski and John J. Gartska, "Network-Centric Warfare: Its Origin and Future," Naval Institute Proceedings.

physical events to measuring the effects of these events in the reason and belief spheres of warfare. Although Lanchester's equations, upon which attrition models are based, captured some important elements of combat, they were applicable only under a large and strict set of assumptions, including having homogeneous forces that are continuously engaged in combat, firing rates that are independent of opposing force levels and are constant in time, and units that are always aware of the position and condition of all opposing units. The equations were deterministic; that is, outputs were directly correlated with inputs. Fuller's moral (belief) and mental (reason) spheres are not directly measured by these MOE. Similarly, the move from attrition warfare to maneuver warfare also poses challenges to the current modeling regime As many of the emerging warfare styles being promulgated by the Services and Joint Staff are maneuver-based (the Army's Precision Warfare, the Air Force's Parallel Warfare, the Navy's Network-Centric Warfare, and the Joint Staff's Joint Vision 2010 concepts), it is unlikely that the current modeling approach (e.g., attrition) will have much applicability.

One tool that holds promise in being able to capture these effects is the Entropy-Based Warfare Model™[3], a model being developed under the auspices of this office. It is based on the paradigm that "warfare can be directed against the cohesion of enemy units or states rather than exclusively against the physical components that comprise those entities."[4] The measure of disorder of the system, not the tally of individual elements destroyed, is the goal of the Entropy-Based Warfare Model™. To this end, the emphasis shifts from force to other factors such as cohesion, friction, and belief factors. The model calculates combat effectiveness as the result of dynamic interactions of physical energy and matter, information, and environmental conditions upon a system.

Next Steps

Based on the thinking behind this paper and its metrics, the authors believe that there are some essential next steps.

1. All experiments should have an hypothesis. In the same vein an experiment should hypothesize metrics and the data required to calculate them. Notional data should then be used to generate the quantitative basis that supports the experiments hypothesis. This type of analysis should drive a Fleet Battle Experiment's data collection plan. Once the experiment is concluded, the data should be run back through the metric tools to generate the real results of the experiment and learn through comparison why the results differed. This approach will increase the value of the experiment.

[3] The Entropy-Based Warfare Model™ was originally developed for the Office of the Secretary of Defense, Office of Net Assessment. The model's purpose is to take extant understanding of the Revolution in Military Affairs (RMA) and build a manual boardgame which allows players to manipulate high sensitivity variables such as space and time to explore RMA organizational and operational concepts. It was initially embodied in a manual simulation (Boardgame) but has since been automated. The automated version has since supported each service's Title X Wargame Series.

[4] Mark Herman, *Entropy Based Warfare: A Unified Theory for Modeling the Revolution in Military Affairs*, white paper, Booz •Allen and Hamilton, 1997, pp 2-3.

2. Develop a more detailed understanding of the attributes and vulnerabilities of the systems that comprise a network-centric force. This needed detail should apply not only to the information and network systems, but also the capabilities of the forces and commanders to make maximum use of the potential of NCW. One way of generating experimental data for use with these metrics is through the conduct of Fleet Battle Experiments. Only by gaining a firmer grasp of the real capabilities can we begin to more accurately measure its effectiveness.

3. Explore the Belief aspects of warfare. There is a consensus concerning the importance of such critical variables as morale, training, experience, leadership, etc. The problem is that analysts and modelers have not yet developed a method for quantifying these predominantly qualitative factors. This has historically been true of warfare aspects such as command and control and the value of information, let alone assessing a soldier's or unit's will to fight. There are some promising measures (training hours, man-hours, etc.) and models (Entropy-Based Warfare, Swarm, etc.) but a great deal more work is required before the analytic community will able to accurately represent these factors.

4. Assess an alternate force structure, based on NCW concepts, which features a move toward increased platform nodes, based on smaller ship classes, whose network creates a virtual capital ship. In the past this concept would have failed because an enemy capital ship would have dominated the smaller non-capital ships. However, with the benefit of the network, the combined capabilities of the ships using the Common Operating Picture would offer alternate force structure options which may optimize the benefits of NCW.

PREFACE

> *"Network-Centric Warfare is at the Leading Edge of a Systemic Transformation with Dramatic and Uncertain Implications."*
>
> Global 98 Executive Session, 31 July, 1998.

Background

As stated by the National Defense Panel, among others, we are in the midst of a Revolution in Military Affairs (RMA). Though the ultimate results are still in doubt, it has become an accepted fact that the information aspect of this RMA will represent a major shift in modern warfare. Revolutions in information warfare, precision strike, space warfare, and maneuver have also been identified, but none of these are possible without the development, incorporation, and integration of information-related technologies.

At the same time, with one notable exception (Nuclear Weapons), RMA's have historically relied upon new operational and organizational concepts to turn nascent technologies into revolutionarily effective military capabilities. The most commonly cited example is the interwar period which witnessed the development of such major operational and organizational innovations as the Blitzkrieg and Carrier Aviation. In each case, the technologies that made the concepts possible (tank, radio, and aircraft for Blitzkrieg; aircraft and aircraft carriers for Carrier Aviation) were extant in World War I, but did not mature until more than a decade later.

Thus, the US Department of Defense has conducted many studies and wargames over the last decade attempting to develop new concepts in accordance with our understanding of the unfolding RMA. Each of the services, as well as the Joint Staff have sought to develop these concepts. Among the most notable of these is Joint Vision 2010 and its call for Full-Spectrum Information Dominance.

The US Navy has spent several years studying the development of information technologies and assessing its potential impact on naval operations. Gradually, the service has begun placing its focus on a concept enabled by advances in information technologies called ***Network-Centric Warfare*** (NCW). To date, the best way to define the concept has been through listing its primary **tenets**:

- Higher echelons provide objectives, timelines, intent, and resource planning.
  - Higher echelons intercede when requests fail to direct resources to respond
  - Higher echelons can veto and re-direct decisions at lower level

- Bottom-up self-synchronizing execution allows all weapons and sensors to be available to all subscribers on the same or linked networks.
  - Request and acknowledgement required across units
  - When request timelines are not met, the request is re-directed to next echelon command element
- A high level of shared awareness enables execution decisions to be coordinated without significant upper echelon intervention.
  - Requires decision makers to receive same intelligence
  - Need intelligent push to avoid overwhelming operators
  - Need intelligent pull to provide auxiliary information to support rapid decision-making
- NCW is effects-based and oriented around human behavior

Still, it is easier and perhaps more instructive to discuss what Network Centric Warfare is not at this point. First and foremost, NCW is not characterized as warfare by networks, or against networks. Instead, it is a concept for conducting warfare more successfully and efficiently through the extensive use of networks to share information and allow for better and more rapid communication and dissemination. Secondly, NCW will not signal the end of the human-in-the-loop, and by extension human error, in warfare. Much like some of the grander claims associated with Dominant Battlespace Awareness (DBA) when it was first discussed in 1994-95[5], there is a tendency to see only the positives in a new concept, and to believe it will solve all the pertinent and age-old problems. A Common Operating Picture (COP), a major facet of NCW, will never ensure that each person viewing the common picture will interpret it the same way, or make a predictable or wise decision to capitalize on the information. Finally, as with DBA before it, it must also be understood that NCW will not abolish Clausewitz's "Fog of War". As long as there is a thinking opponent involved (employing decoys, deception, etc.), no amount of sensor coverage will ever perfectly capture the true situation – regarding either friendly or enemy forces and assets. The body of the paper will provide an even better understanding of NCW's possibilities and limitations at this point in time.

Purpose

The purpose of this paper is to identify and explore the most promising measures of effectiveness for the emerging concept of Network-Centric Warfare. NCW is a US Navy-sponsored concept that will enable the service to increase the efficiency of its forces across the full spectrum of naval missions and operations. This document is not meant to be the definitive analysis of Network-Centric Warfare. Instead, it focuses on

[5] "The emerging system-of-systems promises the capacity to use military force without the same risks before – it suggests we will dissipate the 'fog of war'". Admiral William Owens, "System of Systems", Armed Forces Journal, January 1996, p. 47.

describing metrics for quantifying the efficacy of Network-Centric Warfare once experimental “real world” data becomes available (e.g., Fleet Battle Experiments).

TABLE OF CONTENTS

EXECUTIVE SUMMARY

PREFACE:
- Background
- Purpose

CHAPTER 1: INTRODUCTION

1.1 Network-Centric Warfare
1.2 Network-Centric Warfare: Theory and Implications
1.3 Measuring Network-Centric Warfare
1.4 Metrics Approach
1.5 Conclusion

CHAPTER 2: NETWORK-CENTRIC WARFARE AND THE REVOLUTION IN MILITARY AFFAIRS

2.1 Introduction
2.2 Dimensions of War
2.3 Domains of War
2.4 Theories of War

CHAPTER 3: NETWORK-CENTRIC WARFARE: THEORY AND IMPLICATIONS

3.1 Network-Centric Warfare Background
3.2 Network-Centric Warfare Theory and Tenets
3.3 Implications of Network-Centric Warfare
3.4 Conclusion

CHAPTER 4: MEASURING NETWORK-CENTRIC WARFARE

4.1 Introduction
4.2 System Definition and Characteristics
4.3 Recursive Systems
4.4 Conclusion

CHAPTER 5: OPERATIONAL EXAMPLE

5.1 Introduction
5.2 Generating Battlespace Awareness

5.3 Maximizing Joint Combat Power
5.4 Massing Effects and "Locking Out" Adversary's Courses of Action
5.5 Conclusion

CHAPTER 6: REASON METRICS

6.1 Introduction
6.2 Situational Awareness
6.3 Information Processing and Transport
6.4 Information Warfare
6.5 Conclusion

CHAPTER 7: PHYSICAL METRICS

7.1 Introduction
7.2 Move
7.3 Strike
7.4 Protect
7.5 Conclusion

CHAPTER 8: CONCLUSIONS AND NEXT STEPS
8.1 Key Attributes of Network-Centric Warfare
8.2 Key Metrics
8.3 Navy Integration of NCW
8.4 Next Steps

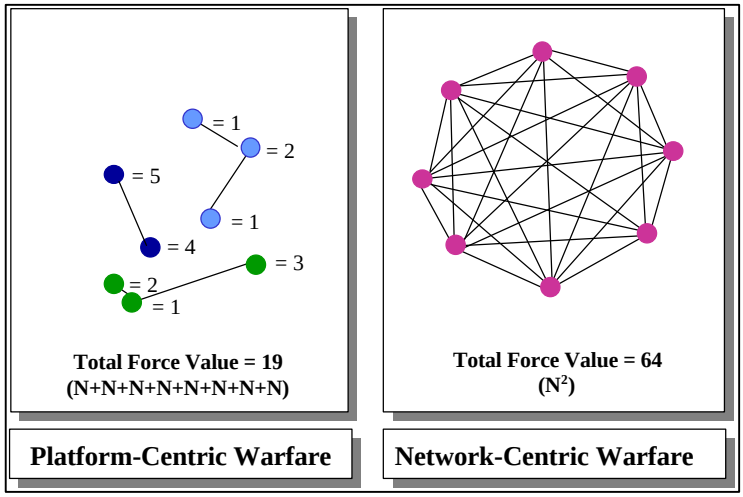
APPENDIX A: BIBLIOGRAPHY

CHAPTER 1 INTRODUCTION

> *"The Revolution in Military Affairs rests more on rapid advances in information and information-related technologies, and less on planes, tanks, and ships."*
>
> National Defense Panel, *Transforming Defense in the 21st Century*

ii. Network-Centric Warfare.

Network-centric warfare suggests that by fighting in a networked condition, we can dramatically increase our combat effectiveness beyond that level obtained by fighting as a collection of individual platforms (i.e., Platform-Centric). In its simplest terms, platform-centric warfare places an emphasis on the platform, or weapons system, as the focal point of combat. A combat platform can be any weapon or system that inflicts physical damage upon an enemy (e.g., tanks, aircraft, artillery, units). Platforms generate combat power. In the Platform-Centric construct, the addition of another platform to a combat formation will usually have an additive effect (e.g., N+N) on combat power; in a Network-Centric Warfare postulate, the inclusion of another node in the distributed network should have an exponential effect (N^N) on combat power[6]. Network-Centric Warfare suggests that a co-evolution of technology, doctrine, and organization will result in a radically different style of warfare, where speed of command, self-synchronization, and the concept of "thin shooters" replaces much of the existing Platform-Centric lexicon.



ii. Theory and Implications of Network-Centric Warfare

Network-Centric Warfare suggests that an inter-woven system of sensor, information, and engagement grids will enable concepts like "thin shooter," "speed of command," and -synchronization" (all defined on page 3-3 and 3-4) and dramatically alter the way in which we conduct warfare. However, in order to isolate and capture the improvements of Network-Centric Warfare to combat operations, these concepts must be measured in the context of the unchanging elements of war. These elements are the dimensions of force, space, and time. These dimensions represent the core elements that have impacted human conflict over the course of known history.

Within this framework, the physical elements -- that is, the movement of men and material, or force, across physical space and time -- have always been emphasized. However, the domain of force is not the only area worth measuring, albeit it is the easiest. The domains of reason and belief are just as important, and may in fact have a greater influence on overall battle outcomes (Napoleon believed that "the moral is to the

[6] N^2 is only valid if the number of nodes is actually very large.

physical as 3 is to 1”). The domain of reason is the realm of human understanding and decision-making. It is the domain of cognition. The belief domain is the realm of organizational behavior. It is the domain of morale, leadership, cohesion, and the willingness to risk life and limb. With its emphasis on time and effects, it is unlikely that improvements promised by Network-Centric Warfare can be captured by analysis and modeling and simulation focused on force and attrition alone. New emphasis on the domains of reason and belief are required.

ii. Measuring Network-Centric Warfare.

To properly capture the impact of Network-Centric Warfare, a modeling and simulation paradigm shift from platform-based to effects-based must occur. In such a shift, traditional metrics of effectiveness, efficiency and robustness are still applicable, although the measures of performance that support these higher level metrics will change. Moreover, the context in which the modeling and simulation occurs needs to be enlarged from measuring purely physical events to measuring the effects of these events in the reason and belief spheres of warfare.

Network-Centric Warfare implies that war should be viewed as a complex adaptive system. It is complex in that it is composed of non-linear interaction of many variables. It is adaptive in the sense that the agents use feedback mechanisms to adapt to and exploit their environment. It is a system composed of hundreds of nested systems and sub-systems that strive to operate as a whole in unison. In order to capture the improvements suggested by Network-Centric Warfare, the modeling paradigm needs to shift from focusing on discrete physical events to capturing larger system effects. While physical measures are still relevant, physical measures alone will not be sufficient to capture the cognitive and behavioral aspects of warfare. A model which incorporates the complex inter-workings of physical force, reason, and belief within a rapidly changing ecosystem needs to be developed. An entropy-based model derived from the field of non-equilibrium thermodynamics appears to offer a better description of complex adaptive systems than classical physics-based force-on-force models.

ii. Metrics Approach.

Quantifying the improvements accruing to Network-Centric Warfare requires new metrics to gauge combat power and new modeling and simulation tools to isolate and capture these new effects. Improvements in warfare have traditionally been measured using the dimensions of force, space, and time. Force improvements are physical enhancements to combat power such as tanks, aircraft, ships and missiles. Improvements in space and time are normally associated with platform speed, range, and speed of command. Although space and time can often be the decisive factors in warfare, most analysis and modeling has focused on the dimension of force exclusively, as it is the easiest to isolate and quantify.

Most prevailing combat models are attrition oriented – that is, they focus on physically destroying the enemy’s military force. Even the most sophisticated force-on-force

models focus on lethality (firepower), tempo (movement and speed), and survivability (protection). In other words, they concentrate on the physical sphere of combat while either ignoring or marginalizing the reason and belief spheres of combat power. Most of these models also ignore or marginalize the dimensions of space and time in favor of an attrition-oriented force model. The operational impact of dominating the dimension of time (i.e., the OODA-loop cycle) and achieving spatial advantage (both physical and virtual) is seldom sufficiently captured in most current force-on-force combat models.

1..1 Reason Metrics.

Reason metrics are the realm of human cognition. They include awareness, analysis, and decision-making capabilities. Reason metrics measure the ability to grasp complex battlefield situations (situational awareness) and to make decisions and act upon them (C^4). Before the collection, processing, and dissemination of information became automated, the contributions of human cognition were difficult to quantify, because they were difficult to isolate. Analysis of human reason tended to concentrate on specific leaders and tactics, emphasizing qualitative rather than quantitative factors. To date, most analysis of the Information RMA concerns the study of modern C^4I systems and decision-making (i.e., the reason sphere) and their operational impact on the weapons systems (i.e., the physical sphere). As emphasis has shifted from individual leadership styles to network architectures and performance metrics, it has become possible to quantify the impact of mental processes on combat power.

1..2 Physical Metrics.

In warfare, physical metrics are divided into three operational areas: Move, Strike, and Protect. Movement involves the ability to transport units and platforms into the battlespace or around the battlespace in order to engage the enemy. Strike is the ability to use direct and indirect weapons against enemy targets. Protect is the ability to prevent, or mitigate the effects, of enemy movements or strikes against friendly forces.

In the physical sphere of warfare, these three operational areas occur within the dimensions of *force, space, and time*. Force is defined as the tangible dimension of military power. It is the lethality or “combat punch” of a particular unit or platform. Space is defined as the position, or distribution, of forces within the ground, air, surface, subsurface, space, cyberspace, and microbial environments. The spatial dimension captures battlespace volume and relative positions of forces. The temporal dimension is reflected in the OODA loop. The concept of the Observe-Orient-Decide-Act (OODA) loop was devised by USAF pilot John Boyd during the Korean War, compressing decision time cycles in order to offset the qualitative advantages of North Korean MIG-15’s. The concept of “speed of command” has its roots in the OODA loop premise, but also incorporates the notions of high rates of change, locking out enemy options, and near-simultaneous and adaptive operations. The time dimension captures the ability to rapidly move and strike against critical enemy nodes, thus creating the shock of closely coupled events and "locking out” enemy actions. Move, Strike, and Protect focus on the application of force within the dimensions of force, space and time.

1..3 Belief Metrics.

The development of belief metrics provides the greatest current challenge in this arena. At this point in the study of the impact of belief in warfare, there is a broad consensus that such factors as morale, experience, and the will to fight of a soldier or unit are the key factors. The importance of these “softer” aspects of warfare has been emphasized for centuries by everyone from Sun Tzu to Napoleon. Their impact is also

easily identifiable throughout history, from the earliest battles to such extreme cases as the Japanese fighting literally to the last man in the Second World War. However, due to its inherently qualitative nature, belief is also the most difficult of the three areas to quantify. In hindsight, key aspects of belief are readily identifiable, when the causality can be at least partially determined. Whether discussing World War I or a NCW-era example, the extent to which morale impacts the effectiveness of a unit is too difficult to predictively measure at this point. Though results concerning belief will be included in the operational example, there will not be a section dedicated solely to a detailed discussion of specific metrics associated with this area as their will be for the reason and physical.

ii. Conclusion.

The Network-Centric Warfare paradigm is based on a series of postulates mapped to the dimensions of force, space, and time and to the physical, reason and belief domains of warfare. While a postulate is a necessary step in decomposing a theory, by definition it is an assumption without mathematical proof as a basis for reasoning. The goal of this study is to provide the analytical basis for Network-Centric Warfare theory and to develop metrics which can be used to prove or disprove the NCW postulates. To this end, this study will review the paradigm shift that lead to NCW, examine NCW within the context of classic factors of combat power, discuss traditional measures of combat power, use physics as an analogy for qualitative and quantitative reasons, and demonstrate how these analogies can be used to develop metrics for NCW. Finally, the study will provide a series of metrics for the reason and physical domains, or spheres, that could be used to measure the contribution of NCW in future modeling and simulation development.

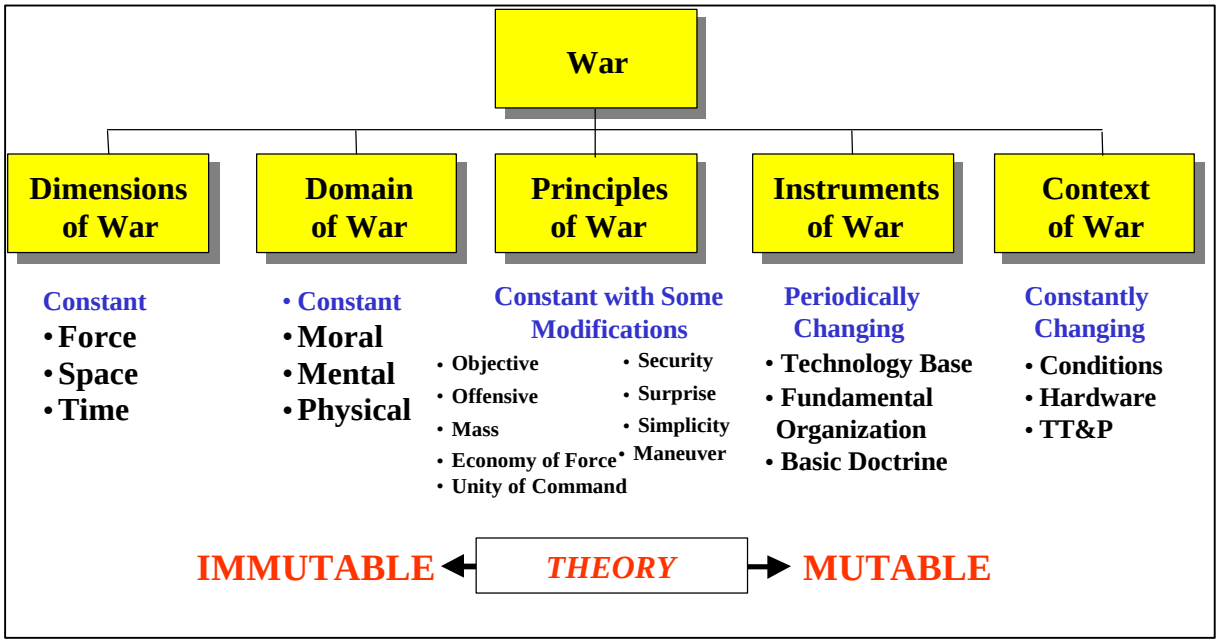
CHAPTER 2 NETWORK-CENTRIC WARFARE AND THE REVOLUTION IN MILITARY AFFAIRS

> *"Scientific revolutions are inaugurated by a growing sense. . .that an existing paradigm has ceased to function adequately in the exploration of an aspect of nature to which that paradigm itself had previously led the way."*
>
> Thomas Kuhn, *The Structure of Scientific Revolutions*

ii. Introduction.

Network-Centric Warfare suggests that an inter-networked system of sensor, information, and engagement grids will enable concepts like "thin shooter," "speed of command," and -syncrhonization" and dramatically alter the way in which we conduct warfare. However, in order to isolate and capture the improvements of Network-Centric Warfare to combat operations, these concepts must be presented in the context of the unchanging elements of war: the physical dimensions of force, space, and time, and together with the domains of belief and reason.

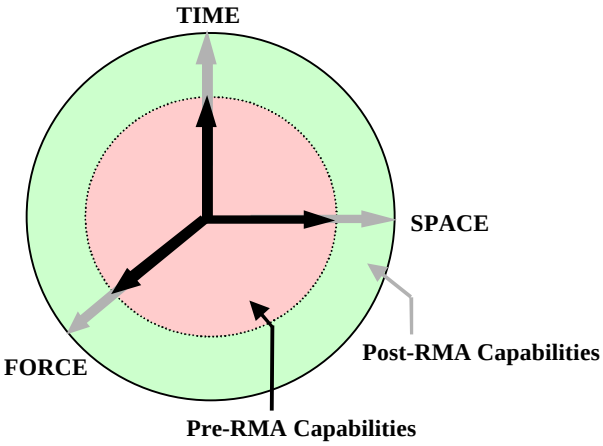
Sometimes technological changes, coupled with new organizations and doctrine, fundamentally transform warfare. The concept of a Revolution in Military Affairs is based on this idea. The current Information-based RMA, driven by quantum increases on microchip speed and network performance, stresses the value of accurate, timely and relevant information, networked capabilities, information architectures, and long-range precision fires and maneuver.



Warfare is a mixture of unchanging and changing elements linked by theories that attempt to bridge the gap between these elements. Revolutions in Military Affairs include the changing elements of hardware, tactics, techniques and procedures, technology base, organizational and process changes, and, to a certain extent, modifications to the principles of war. However, the RMA must still be viewed within the context of the unchanging elements such as the dimensions and domains of war.

ii. Dimensions of War.

Radical transformations in combat effectiveness are contingent upon simultaneous order-of-magnitude improvements in the dimensions of force, space, and time. Measuring improvements to military operations is predicated on isolating and quantifying improvements in each of these dimensions. We are currently in a gray zone between the pre-RMA and a post-RMA environment. This gray zone represents a slow paradigm shift that will ultimately expand the dimensions of force, space and time in a post-RMA battlespace.

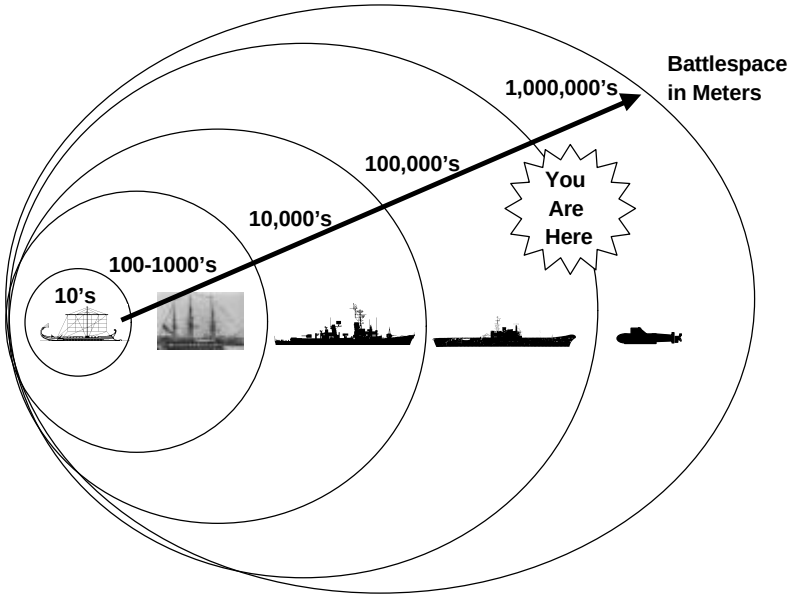


2..1 Force.

Force is defined as the tangible dimension of military power. It is the lethality or "combat punch" of a particular unit or platform In warfare, improvements to force have included the introduction of gunpowder, battleships, aircraft and precision-guided munitions, to name of few. Information improves the effectiveness of kinetic weapons, especially long-range, GPS-guided ones. Timely and accurate information exchange between sensor and shooter increases the probability of locating, classifying, and hitting the desired target (P_{hit}). In turn, the increase in individual weapon effectiveness results in a net increase in potential force. In the past, force was measured in terms of sheer mass; in the future, force will be measured more in terms of precision effects.

2..2 Space.

Improvements in information technologies and telecommunications has radically altered the spatial aspect of warfare, creating a paradigm shift from centralized to distributed operations. The spatial dimension captures battlespace volume. It includes the three-dimensional Euclidean space of forward/backward, left/right, and up/down. In the past, the introduction of the horse, railroad, automobiles, aircraft, and telecommunications have radically altered spatial relationships in the battlespace. As military transportation and communications capabilities have grown so has the geographical area of responsibility and spatial disposition of combat units. For example, since World War II, the area of responsibility for a division-sized unit in the US Army was grown from 40 square kilometers to the 24,000 square kilometers planned for Division XXI in 1999. Likewise, the battlespace for a naval battlegroup has expanded from hundreds to thousands of kilometers since World War II. As the battlespace has increased, the combat organizations charged with responsibility for these battlespaces have actually become smaller.



In the information-based RMA, a disaggregated network of sensors, command centers, and weapon systems allows for greater dispersion of combat forces while maintaining situational awareness, thus enabling greater mobility and survivability. Greater dispersion generates increased complexity for the enemy commander and decreases his overall understanding, while networked systems offer simplicity and greater understanding for the friendly force commander. Information technologies and telecommunication systems are primarily responsible for this move from a linear to a non-linear battlespace. In the past, overcoming the problems associated with space was mainly a factor of physical speed (i.e., how much distance a particular force could cover over time); in the future, space will be measured in terms of information (situational awareness), indirect weapons range, and physical speed of units and platforms. The emphasis is shifting from physical speed and presence to virtual speed and presence. This is the key to understanding the spatial dimension.

2..3 Time.

Although information technologies make significant contributions to force value, the real benefit of information is in the temporal and spatial aspects. The temporal dimension of warfare has contracted rather than expanded. In the industrial age, time references shrank from months and weeks to days and hours. In the information age, time references have moved to seconds and nano-seconds. The ability to act in the shortest time in warfare promises a decisive edge in combat operations. For example, operations for both sides during the Revolutionary War were planned and conducted over the course of a season. Allied operations during the gulf War were planned and conducted during the course of a single day. This temporal compression was articulated and employed as an advantage during the Korean War, when Boyd's Observe-Orient-Decide-Act (OODA) loop was used to compress decision cycle time in order to offset force advantages of North Korean MIG-15's.

2..4 Historic Example.

Operations based on the concepts of force, space, and time have well attested historical precedents. Perhaps the best example is the German Blitzkrieg during World War II. German forces utilized existing technologies such as tanks, aircraft, and radios and coupled them with changes in doctrine and organization, providing the German army a decisive edge over Allied armies. German troops combined this force advantage (combined arms warfare with direct air support) with a principle of decentralized command (*auftragstaktik*) to gain spatial and temporal advantages over the Allies. Under decentralized command, German armies successfully avoided massed allied formations (surfaces) and attacked lightly defended points (gaps) with a final concentration of force at a decisive point (*schwerpunkt*). This effective and efficient exploitation of force, space, and time greatly compressed German operations (victory over the British and French forces was achieved in 40 days) and reduced causalities. For the

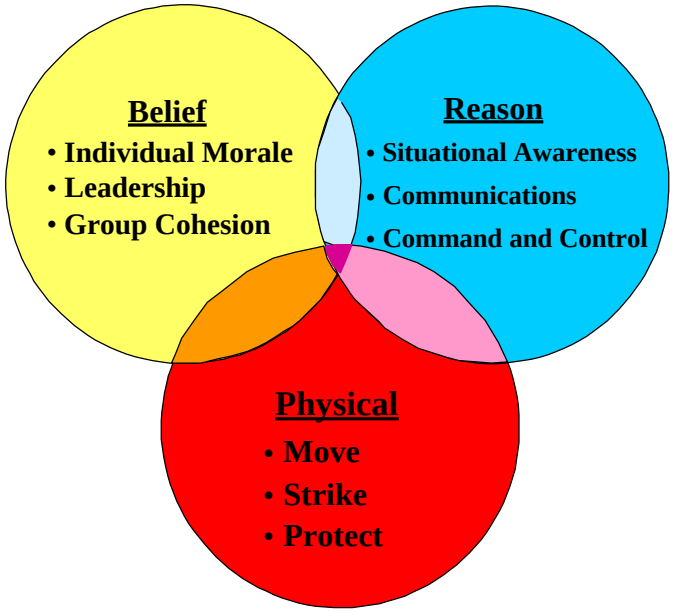
Revolution in Military Affairs, the key point is this: German forces achieved such lopsided victories only through a co-evolution of process and organizational change with technological innovation against opponents who did not develop a similar process.

2..5 Dimensions of War Summary.

The use of force, space, and time is more than an analogy for measuring physical combat power. It is a model for developing Network-Centric Warfare metrics. The dimension of force, as expressed by precision and lethality, can be measured; the amount of space that a combat unit can cover can be measured; and the amount of time it takes to perform a combat function can be measured. Further refinements to these measures can be made where two of these dimensions intersect (e.g., improvements to both tempo and lethality). In essence, the dimensions of force, space and time can yield at least six different measures of combat power: force, force/time, time, time/space, space, and space/force.

ii. Domains of War.

In 1917, J.F.C. Fuller, a British military officer and historian, delivered a lecture outlining the basic principles of war. Fuller based these principles upon three interrelated spheres; mental, moral, and physical.[7] *Fuller's mental sphere equates to the reason domain, and the moral sphere equates to the belief domain.* Fuller emphasized the need to "think of war scientifically", to quantify the effects of combat power. Fuller emphasized the physical aspects of combat power through the destruction of the enemy's physical strength. According to Fuller, "destruction of the enemy's physical strength is the canon of the physical school of war." He realized that the moral (belief) and mental (reason) spheres were crucial, but were intangible and difficult to quantify. Therefore, great emphasis was placed on evaluating the physical sphere. Combat power is characterized by the confluence of the three basic elements of physical, moral (belief), and mental (reason). These three areas are not mutually exclusive but rather complement each other. Traditionally, the physical element has been emphasized more because it is the easiest to quantify; however, the moral and mental forces exert a greater influence on the outcome of war.



2..1 Physical.

The physical sphere is the easiest to isolate and measure since it generally focuses on tangible items such as equipment type, capabilities, and disposition. In warfare, the physical sphere is divided into three activities: move, strike, and protect. Movement involves the ability to transport units and platforms into the battlespace or around the

[7] J.F.C. Fuller, "The Foundations of Science and War"

battlespace in order to engage the enemy. Strike is the ability to use direct and indirect weapons against enemy targets. Protect is the ability to prevent the enemy from moving against or striking friendly forces. The physical sphere can be measured by isolating such areas as weapons effectiveness (e.g., probability of kill), loss-exchange ratios, friendly survivability, or tons delivered per day.

2..2 Reason.

Reason, similar to Fuller's mental sphere, includes awareness, analysis, and decision-making capabilities. It is the ability to grasp complex battlefield situations (situational awareness) and to make decisions and act upon them (C^4I). Historically, contributions of reason have been difficult to quantify. Instead, analysis of reason has tended to concentrate on specific leaders and tactics, emphasizing qualitative rather than quantitative factors. To date, most analysis on the Information RMA concerns the study of modern C^4I systems and decision-making (i.e., reason) and their operational impact on the weapons systems (i.e., physical). The emphasis has shifted from individual leadership styles to network architectures and performance metrics. Consequently, it has become possible to isolate and quantify the impact of mental processes on combat power. Collection and processing can be modeled and quantified using ISR analysis tools and dissemination means can be optimized using network analysis tools such as OPNET.

2..3 Belief.

Belief includes individual morale, leadership, group cohesion, resolve, emotion, fear, training, experience, etc. If reason involves human cognition, then belief involves cohesion. Where the implementation of reason in information warfare is a battle for the enemy's *mind*, the goal within the belief sphere is destroy the enemy's will by underscoring the impact of his losses and the hopelessness of his situation. Although the components of belief are perhaps the most significant element of combat power, they have been the most difficult to isolate and quantify. The goal of the unit commander is to increase his unit's cohesion (and, hence, effectiveness) while decreasing the cohesion of enemy units through such tactics as maneuver operations, psychological operations, and mass bombing to campaigns. Time is an important dimension within the belief sphere as weaknesses in unit cohesion and individual morale are normally temporary and can be remedied by higher echelons over time.

2..4 Historic Examples.

Historically, reason and belief have figured prominently in victory and defeat. Although the physical domain affects both reason and belief, physical effects alone—short of annihilation – have not proven to be the decisive factor in victory or defeat. In a study conducted by the US Army Concepts Analysis Agency, the psychological effects of maneuver by the enemy represented sixty percent of the reasons a force abandoned an attack or defense. Included in the areas of maneuver were envelopment, encirclement, penetration (33%), adjacent friendly unit withdrawal (13%), enemy key terrain advantage (6%), and the element of surprise (8%). Physical losses in the form of causalities and equipment accounted for only ten percent of the reason for abandonment.[8] In a study on the air-to-air combat experience in Southeast Asia during Operation Linebacker, the element of surprise was the most important factor affecting the loss of both US and Vietnamese fighter aircraft. Lack of knowledge or time-late awareness of enemy presence accounted for 81% of all fighter losses.[9] An effort to emphasize reason and belief is important because most analysis, modeling and simulation focus primarily on the physical domain of war in the form of loss-exchange ratios and weapons performance. Despite their acknowledged critical roles, behavioral and

[8] US Army Concepts Analysis Agency, "Causes for Defeat in Battle (1941-1982)"
[9] Project Red Baron II, Vol. III, Pt.1, p. 61.

cognitive areas are either ignored or extrapolated from physical outputs (e.g., the fifty percent attrition rule).

ii. Theories of War.

There have been two historically dominant theories of warfare: attrition and maneuver. Although new technology and tactics may change the vocabulary involved, most theories of warfare can be traced back to either attrition or maneuver styles. The distinction between these two theories is very important to modeling and simulation because most current models are mainly attrition-based. As many of the emerging warfare styles being promulgated by the Services and Joint Staff are maneuver-based (the Army's Precision Warfare, the Air Force's Parallel Warfare, the Navy's Network-Centric Warfare, and the Joint Staff's Joint Vision 2010 concepts), it is unlikely that the current modeling approach will have much applicability.

2..1 Attrition Warfare.

Attrition warfare focuses on grinding down the enemy through superior resources and numbers. Attrition warfare achieves victory eroding their strength with superior mass and killing power and annihilating them through complete destruction and occupation. Although attrition warfare is generally associated with agrarian era warfare and has acquired a negative reputation, it has been used quite successfully in the industrial era, as evidenced by the Northern victory in the American Civil War and the Russian WWII victory against a maneuver-oriented German Army. Attrition warfare centers locating and destroying a series of targets with the aim of obliterating the enemy's material strength. In the dimensions of force, space, and time, attrition warfare is primarily concerned with the aspect of force and increasing its force advantage vis-à-vis the enemy. Under attrition warfare, mental disruption and moral collapse are secondary or tertiary effects of massive physical destruction.

2..2 Platform-Centric Warfare.

Platform-centric warfare has dominated warfare throughout the 20th century. In its simplest terms, platform-centric warfare places an emphasis on the platform, or weapons system, as the focal point of combat. A combat platform can be any weapon or system that inflicts physical damage upon an enemy (e.g., tanks, aircraft, artillery, units). Platforms generate combat power. The ability of this combat power to inflict physical damage, or attrition, forms the basis for military organization, doctrine, tactics, techniques and procedures.

Platform-centric warfare is a direct combat power approach with an objective to qualify and quantify combat power through analysis of the platforms that directly generate power. Each platform, or object, is assessed to possess a measurable degree of combat value. This combat value reflects the lethality of an object relative to another object on the battlefield. The result of platform confrontation is attrition, with one or more sides suffering physical damage. The attrition-based paradigm lends itself to numerical force comparisons to determine the relative combat strength, or capability, of opposing forces. These numerical comparisons are often expressed as force ratios, which serve as a predictor of combat attrition outcomes. If the combat power of force "A" can be measured and compared to the combat power of force "B", then attrition-based algorithms can predict probabilities of successful engagements. This approach has led to

doctrinal development for maneuver and fires based upon force ratios required for offensive and defensive operations, such as over running opposing forces (the so-called "3:1 ratio), falling-back to defensive positions, etc. Strategy has been refined to mass maneuvering forces at decisive points to achieve favorable local force ratios for armored breakthroughs. Artillery tactics have been used widely in this century based upon concentrating fires at the center of mass to increase attrition and destruction of enemy forces (i.e., platforms).

Platform-centric warfare information architectures are characterized by hierarchical information flows, voice communications, limited interoperability, and stove-piped battle management systems for fires, air defense, strike, intelligence, and combat support. The information technology architectures in platform-centric warfare are designed to support industrial-age organization and processes. This paradigm has led to rigid, top down hierarchical organizations emphasizing centralized planning and coordinated execution across a contiguous battle front. The emphasis in platform-centric warfare is not temporal or positional advantages, but force.

2..3 Maneuver Warfare.

Maneuver is strictly defined in Joint Publication 1.02 as the "employment of forces on the battlefield through movement in combination with fire, or fire potential, to achieve a position of advantage in respect to the enemy in order to accomplish the mission." However, maneuver is more than simply achieving positional advantages: its primary goal is to generate systemic disruption and create enemy friction through rapid, violent attacks against key centers of gravity. Maneuver is built on the tenets of preemption (defeating or neutralizing the enemy before the fight), dislocation (rendering the enemy's strength irrelevant by removing the enemy from a decisive point in function, space, or time), and disruption (neutralizing the enemy by successfully attacking or threatening his center of gravity). If attrition warfare is focused on physical effects, maneuver warfare is primarily concerned with reason and belief effects, the so-called "intangibles" of war. While force is still an important dimension of maneuver, it is the concentration of that force in space and time that is most critical. Consequently, maneuver is measured in terms of speed and surprise, not in terms of firepower alone.

CHAPTER 3 NETWORK CENTRIC WARFARE: THEORY AND IMPLICATIONS

.

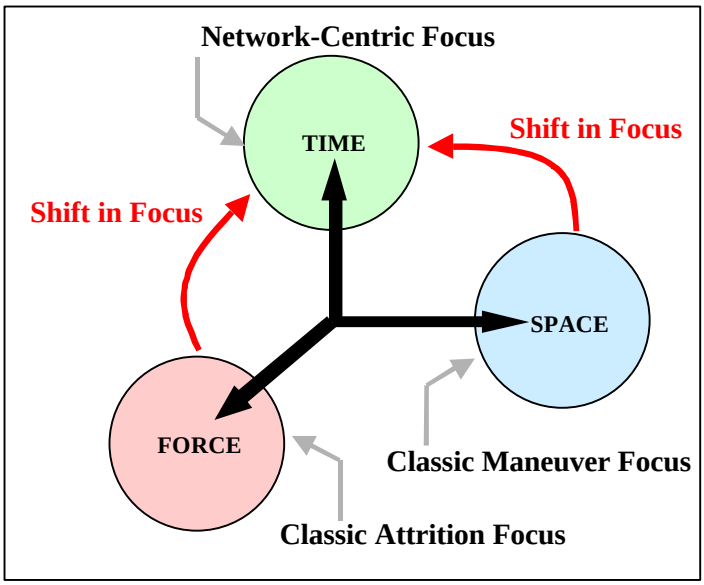
> *"Networks are created not just to communicate, but also to gain position, to out-communicate."*
>
> G.J. Mulgen, *Communications and Control: Networks and the New Economies of Communication*

ii. Network-Centric Warfare Background.

Network-Centric Warfare is largely derived from the advent of network-centric computing in the business world. During the 1960s and 1970s, most information technology workers within a department or company were dependent on one centralized processor for computing power and user applications. The mainframe era was characterized by expensive processors and proprietary software, requiring highly skilled technicians to operate and maintain these systems. This *mainframe-centric* approach started to fade in the 1980s with the advent of the microprocessor, personal computer, and commercial software explosion. Homogenous operating systems of the mainframe era were replaced by heterogeneous operating systems and application programs of the PC era. Simplified operating systems and applications increased accessibility to computing power and made computer users less dependent upon centralized information systems. However, the plethora of new operating systems, incompatible software, and continuous upgrades in the *PC-centric* era decreased interoperability and often increased the complexity of communicating between two different computing platforms.

In the mid-1990s, the PC-centric view shifted towards a *network-centric* paradigm. This paradigm emphasized distributed computing environments where applications and data were downloaded locally from network servers on an as-needed basis, utilizing high bandwidth pathways and low cost "thin" clients. In this paradigm, higher cost personal computers (which become obsolete within 18 months) are replaced by lower cost Network Computers (NC, the so-called "thin" client). Network Computers normally have the same processing power of a PC but fewer options. Network-centric computing became more than technological enhancement: it changed the fundamental paradigm of conducting business. Network technologies and radical processing reengineering offered supplier-to-customer linkages, decentralized decision-making, enabled distributed operations (e.g., the virtual office), and dramatically compressed the business planning cycle from months to days. Technological improvements radically altered existing business concepts of time and space, changed organizational structures and behavior, and fundamentally transformed traditional business processes.

In network-centric computing the measure is no longer how many users per computer, but how many computers per user. The result is a Revolution in Business Affairs (RBA) -- a paradigm shift from hardware-centric to a network-centric environment which emphasizes Metcalfe's law (the value of a network increases exponentially as the number of users increases while networking costs increase linearly) over Moore's law (the number of transistors that can fit on a chip doubles every 18 months). Just as the RBA is enabled by the transition from hardware-centric to network-centric computing, the RMA is enabled by the transition from platform-centric to network-centric warfare. Network-Centric Warfare emphasizes the value of the platform in the networked condition over traditional platforms in contributing to operational effectiveness. NCW is based on the Net-Centric computing concept, but also requires, and enables, an effective human element performing collaborative thinking, planning and reacting. NCW's ability to rapidly share information also promises significant improvement in a commander's ability to access a variety of reachback knowledge and data.



[11].

Network-Centric Warfare will be enabled by a series of inter-netted grids. These grids will link sensors, battle commanders, and weapon systems. The information grid will provide the communications and computing back-plane. The sensor grid will link all sensors in the battlespace to generate battlespace awareness and synchronize battlespace awareness with combat operations. The engagement grids will exploit the battlespace awareness provided by the sensor grid to maximize Joint combat power and mass effects versus massing forces. However, Network-Centric Warfare will only be a force multiplier when its technical capabilities are matched by a co-evolution of operational concepts, organizations, and doctrine.

3..1 "Thin Shooter".

The "Thin Shooter" concept is derived from net-centric computing practices. These practices move from traditional host/terminal environments of mainframes toward a distributed client/server computing environment composed of low-cost access terminals (i.e., the "thin client"). The shift from the platform to the network offers new options on how forces and platforms could be constructed to perform the same set of missions more effectively and efficiently. The "thin shooter" concept moves from the capital ship-centric organization of the Carrier Battlegroup to a distributed "virtual cap composed of stealthy, swift and modular surface and sub-surface combatants. These smaller, dispersed combatants can gain both maneuver and temporal advantages thanks to internetted information available. This will allow them to generate the required firepower at the critical point without having to rely upon the heavier, more observable

[10] VADM Arthur K. Cebrowski, "Sea Change," *Surface Warfare*, November/December 1997, p. 4
[11] VADM Arthur K. Cebrowski and John J. Gartska, "Network-Centric Warfare: Its Origin and Future," Naval Institute Proceedings,

do?”), and Act (“Inform my subordinates and execute”) cycle, a military commander can use initial information superiority to rapidly attack critical enemy nodes, thus creating the shock of closely coupled events and "locking out” enemy options. By quickly assessing and adapting to a complex battle environment, the commander can exploit the initial conditions and “drive” the enemy commander’s battle plan by a series of discrete and predictive engagements. “Speed of command” develops a very high and accelerating rate of change, locking out enemy strategies and options by operating within their Observe-Orient-Decide-Act (OODA) loop. Speed of command offers a force multiplying capability that could offset numerical, technical, or positional disadvantages, as well as the ability to closely couple a variety of operations across great distances. The emphasis shifts away from force toward time and position. This is the hallmark of Network-Centric Warfare. Efficient information technologies and effective process reengineering can reduce the OODA cycle from days and hours to minutes and seconds. Thus, increased tempo is one of the key tenets of Network-Centric Warfare.

3..3 “Self-Synchronization”.

“Self-synchronization” of forces promises to more efficiently use combat power by enabling bottom-up organization through timely, relevant and accurate information coupled with commander’s intent that fosters maximum freedom of action. Adaptivity is a key component of “self-synchronization.” Each node in the network may function as a non-linearly interacting component, giving rise to a whole (the network) that is greater than the sum of its parts (the nodes). “Self-synchronization” is related to the concept of self-organization, which views actors as part of a continuously adapting ecosystem rather than disconnected platforms. In this sense Network-centric ideas are rooted in the science of complex systems and complexity theory. Complexity theory, as it relates to network-centric warfare, is a general approach to understanding the overall behavior of a system composed of many non-linearly interacting parts. It is predicated on the following premise: the system's behavior owes at least as much to how the system's parts all *interact* as to what those parts are. “Complex behavior" is usually an emergent self-organized phenomenon built upon the aggregate behavior of many non-linearly interacting "simple" components. The ability of these parts to self-organize around relevant information in a changing and complex battlespace provides a competitive advantage to the side that masters Network-Centric Warfare.

ii. Implications of Network-Centric Warfare.

The implications of Network-Centric Warfare are immense and include all dimensions and domains of warfare. Information commonality and velocity may increase a force commander’s course of action options, thus providing greater flexibility and adaptability. Precision information in the Network-Centric Warfare environment translates into precision engagement capability and asymmetric force advantages. A networked environment could enable swarm-like attacks against the enemy through concepts like “digital *schwerpunkt*” and “self-synchronization.” Through physical and mental agility, the blue force commander can disrupt enemy tempo, achieve “lock-in,” and limit the enemy commander’s courses of action. Through synchronized physical and information assaults, a commander could destroy enemy cohesion, rapidly defeating the enemy without resorting to attrition-style campaigns. Increased physical and mental

adaptability will allow force commanders to adapt to, and exploit, the rapidly changing battlespace, leveraging friendly force "fitness" while increasing the enemy's friction.

ii. Conclusion.

Adherence to a given theory of warfare is an important part of determining what kind of metrics to employ in combat models. Proponents of attrition theory emphasize the importance of killing lots of objects on the battlefield, tallying the numbers for both sides, and formulating loss-exchange ratios to calculate warfighting improvements. Most combat models employed today are formulated on this hypothesis. With the exception of elements like physical fatigue, areas such as mental disruption and system collapse are seldom addressed in attrition-based models. Network-Centric Warfare emphasizes the systemic nature of warfare, in which the physical, reason, and belief spheres are closely coupled. Network-Centric Warfare is non-linear in nature; input (the amount of enemy platforms destroyed) is not necessarily proportionate to output (mental disruption and moral collapse). Network-Centric Warfare views the enemy as a complex system of interrelated parts which have different relationships and values depending upon their function in space and time. Unfortunately, the models currently used to determine improvements to combat power are based on classic physical measures of power. It is unlikely that attrition-based models will fully capture the impact of parallel, precision, or Network-Centric Warfare.

CHAPTER 4 MEASURING NETWORK-CENTRIC WARFARE

"The moral is to the physical as three is to one."

Napoleon

ii. Introduction.

In order to properly capture the impact of Network-Centric Warfare, a paradigm shift from platform-based to effects-based modeling and simulation must occur. Traditional metrics of effectiveness, efficiency and robustness are still applicable, although the measures of performance that support these higher level metrics will change. Moreover, the context in which the modeling and simulation occurs will need to be enlarged from measuring purely physical events to measuring the effects of these events in the reason and belief spheres of warfare. The classical mechanics approach used to measure force value will need to include the non-equilibrium thermodynamics approach of measuring system state changes.

ii. Metrics: Definition and Characteristics.

Metrics are analytical devices used to measure improvements to a system. At the generic level, metrics can be divided into three areas: *effectiveness, efficiency, and robustness*. *Effectiveness* quantitatively captures the intended or expected results of systems or operational improvements. *Efficiency* is the ratio of work accomplished or energy expended relative to material inputs or time. In short, it is the accomplishment of a task with minimum expenditure of time and effort. *Robustness* is a measure of the overall health of a system. It implies the ability to avoid or absorb damage with minimum operational impact. Robustness is normally associated with depth, strength, and redundancy.

Metrics are traditionally divided into two basic categories: Measures of Effectiveness (MOEs) and Measures of Performance (MOPs). A MOE is a quantitative indicator of a human, human/materiel, or materiel system to accomplish the mission for which it was designed. For a military force, it is a measure of the ability of the force to accomplish its combat mission -- that is, its combat or operational effectiveness. MOE are system or force attributes used to evaluate the ability of alternative approaches to meet functional objectives and mission needs. Examples of such measures include loss exchange results, force effectiveness contributions, and tons delivered per day.

An MOP is a quantitative indicator of the performance capabilities of a system. MOP are system attributes that measure how the system/individual performs its functions in a given environment (e.g., number of targets detected, reaction time, number of targets nominated, susceptibility of deception, task completion

time.) It is closely related to inherent parameters (physical and structural), but measures attributes of system behavior.[12]

ii. The Traditional Approach of Assessing Combat Effectiveness.

4..1 Lanchestrian Measures.

Much current modeling employs mathematical equations developed by Frederick W. Lanchester in the early 20th century to calculate casualty and attrition rates. Lanchester introduced a set of coupled ordinary differential equations as models of attrition in modern warfare. Although Lanchester's equations captured some important elements of combat, they were applicable only under a large and strict set of assumptions, including having homogeneous forces that are continuously engaged in combat, firing rates that are independent of opposing force levels and are constant in time, and units that are always aware of the position and condition of all opposing units. The equations were deterministic; that is, outputs were directly correlated with inputs.

Fuller's moral (belief) and mental (reason) spheres are not directly measured by these MOE. In order to circumnavigate this Lanchester-based limitation, creative methods have been developed in an attempt to capture the effects of unit cohesion and command. Examples include the effects of information velocity on human decision-making, speed of command effects, improvements in situation awareness through information commonality, shock and awe factors, and weighted values for training and readiness factors. However, the outcome from all of these modifications ultimately returns to attrition-based MOE. More targets are destroyed faster, less resources are expended, objectives are attained faster, blue losses are reduced, and so on. MOE and MOP do not exist in the current family of models to quantify and capture the "intangible" effects of reason and belief. This is the key limitation of Lanchester-based combat models.

Numerous attempts have been made to incorporate the notion of Clausewitzian friction into models, but these efforts have ultimately derived from weapons performance and firepower data. Other approaches attempt to build hierarchical constructs which base the behavior of less detailed models on the output of more detailed models. The problem with the latter approach is that the less detailed, higher level models are calibrated by detailed attrition models; thus, the detail being added to the higher level model is simply more specific weapons performance data with inter-visibility calculations added. Alternate approaches attempt to factor in some of the soft factors of intelligence through the development of targeting data within the command control system. [13] The shortcoming of this approach is that it limits the use of intelligence almost exclusively to the purpose of more accurately applying weapons against targets.

The basic idea behind these equations is that the loss rate of forces on one side of a battle is proportional to the number of forces on the other. In one form of the equations, known as the directed-fire (or square-law) model, the Lanchester equations are given by the linear equations:

$$b[B(0)^2 - B(t)^2] = r[R(0)^2 - r(t)^2] \text{ or}$$
$$dR(t)/dt = -\alpha_B B(t) \text{ and } dB(t)/dt = -\alpha R\, R(t)$$

where R(t) and B(t) represent the numerical strengths of the red and blue forces at time t, and αR and αB represent the constant effective firing rates at which one unit of strength on one side causes attrition of the other side's forces.[14] The deterministic and stochastic Lanchester equations for direct and indirect fire are used for both homogeneous and heterogeneous forces. In current Lanchestrian equations models of combat, engagements, instead of being fought with individual entities, are abstracted using a stochastic method in the form of a combat results table (CRT) or through Lanchester equations for force attrition

[12] TRADOC Pamphlet 71-9
[13] Steven C. Bankes, Methodological Considerations in Using Simulation to Assess the Combat Value of Intelligence and Electronic Warfare, (Santa Monica: RAND Corporation, 1991), p. 16.
[14] Andrew Illachinski, "Land Warfare and Complexity"

Lanchester's equations have subsequently become the seminal source for all attrition-based modeling development in the 20th century. Following from the classical mechanics metaphor, these equations apply Newtonian principles to the measurement of combat outcomes. Lanchester's equations are used to model combat as a deterministic process, based upon "attrition-rate coefficients". The static equations do not take into account external factors, such as terrain effects, suppression fire effects, spatial and temporal variations between forces, human psychological factors, and decision-making capabilities. Lanchester equations are well suited to measuring pure force, but do not capture the dimensions of space and time. Being rigid and deterministic, these equations failed to model real world combat, in large part because they lack spatial and temporal degrees-of-freedom.

While there have been many extensions to and generalizations of Lanchester's equations over the years, very little has really changed in the way we fundamentally view and model combat attrition. While the Lanchester equations are particularly relevant for the kind of static trench warfare and artillery duels that characterized most of World War I, they are too simple and lack the spatial degrees-of-freedom needed to realistically model modern combat. The fundamental problem is that they idealize combat much in the same way as Newton's laws idealize the real chaos and complexity of the world.

The theme of measuring relative physical combat power was not fully realized until the 1960's, when systems analysis techniques were first applied to determine force ratios. In 1976, the new version of Army Field Manual 100-5 made repeated references to force ratios derived from these systems analysis techniques. Force ratios were determined using Lanchester's equations in order to predict the results when two forces fought. As a result, the quantifiable aspects of attrition warfare were emphasized at the expense of the intangible spheres of reason and belief factors.

The emphasis on physical destruction results in measurements to determine the probability of destroying, or killing, the target. A Probability of Kill (P_{kill}) became the standard measurement for success, or failure, of a particular weapon system. P_{kill} percentages have been developed for all joint munitions, and have become standardized in the Joint Munitions Effectiveness Manual (JMEM). JMEM data is used widely in all current combat models to evaluate and compare munitions effectiveness against particular target sets. MOE have been developed based upon these P_{kill} percentages.

A classic example of this practice is the Loss Exchange Ratio (LER). This MOE compares enemy losses to friendly losses and expresses the result as a ratio. LER determination is solely attrition-based, summing the amount of human casualties or materiel destroyed. Based upon this MOE, force ratios are determined and used as a predictor of successful combat outcomes. The traditional 3:1 force ratio required for offensive operations is a result of this type of analysis. Other attrition-based MOE examples include types of targets destroyed, number of targets destroyed by target type, munitions effectiveness by weapon type (e.g., artillery effectiveness, naval surface fire effectiveness), resource expenditure, units rendered combat effective, etc.

4..2 Lanchestrian-based Models.

A wide variety of models have been developed over the last 30 years to analyze warfare across many different mission areas. Current combat models are based upon Lanchester's equations and are attrition-based. The models used today are primarily deterministic, using a linear cause and effect within a closed simulation. These combat models range from item-level tactical models to force-on-force operational and theater models. Each Service has developed their own unique models to evaluate a particular niche of warfare. As a result, hundreds of combat models have proliferated the community, each designed to capture the physical sphere of a particular mission area, such as air defense, air superiority, ground maneuver, etc. All of these models use physical force as the primary discriminator, and MOE are not well developed in the spatial and temporal spheres.

Traditionally, simulations of complex systems have consisted of mathematical or stochastic models, typically involving differential equations, that relate one set of global parameters to another set and

describe the system's overall dynamics. The behavior of a system is then "understood" by looking at the relationship between the input and output variables of the simulation. While such a deterministic approach is adequate for systems with parts that possess little or no internal structure, it is largely incapable of describing groups, or societies, in which the ***internal dynamics*** of the constituent members of the system represent a vital part of the underlying dynamics. This is a shortcoming of the Lanchester attrition-based approach to modeling and simulation.

Prevailing combat models have consisted of firepower, maneuver, and survivability. These three areas comprised the physical sphere of combat power. Other areas such as reason, belief, and leadership were either ignored or marginalized in favor of the physical sphere, which could be quantified through deterministic Lanchestrian equations where input was roughly equal to output. Network-Centric warfare emphasizes the non-physical sphere of warfare such as leadership, morale, and information. In this light, the physical-based Lanchester model does not effectively capture the impact of information, leadership, and moral functions on battle outcomes.

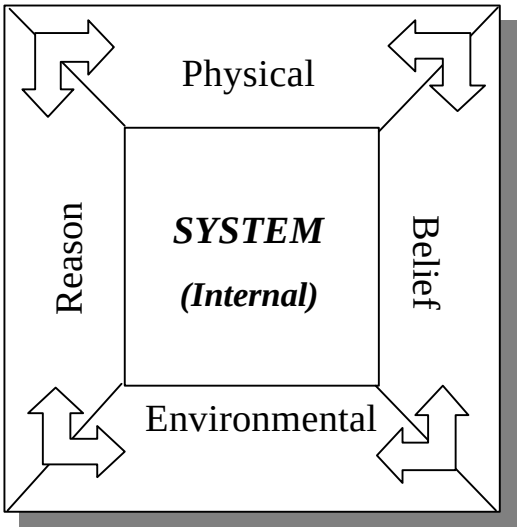
ii. Paradigm Shift: From Centralized to Decentralized Models.

Most current measures of combat are based on force enhancements to the physical domain of war, where cause and effect exhibit a linear relationship. The Newtonian paradigm of linear cause and effect, where one object (the controller) acts on another object (the receiver) and influences the motion of that object, has dominated combat analysis and modeling for decades. Interestingly, Newton's Third Law which states that for every action there is an equal and opposite reaction, is de-emphasized in most models. The reaction principle in Newton's Third Law forms the basis of decentralized interactions and feedback mechanisms. The principle also necessitates a shift from viewing the isolated interactions of individual elements to focusing on the emergent behaviors of systems. A systems approach offers a more realistic way of modeling the behavior of complex ecosystems, where cause and effect have a non-linear relationship. The movement from measuring individual elements to measuring systems in combat modeling reflects a paradigm shift from *platform-based modeling* to *effects-based modeling.*

ii. The Systems-based Approach of Assessing Combat Effectiveness.

4..1 System Definition.

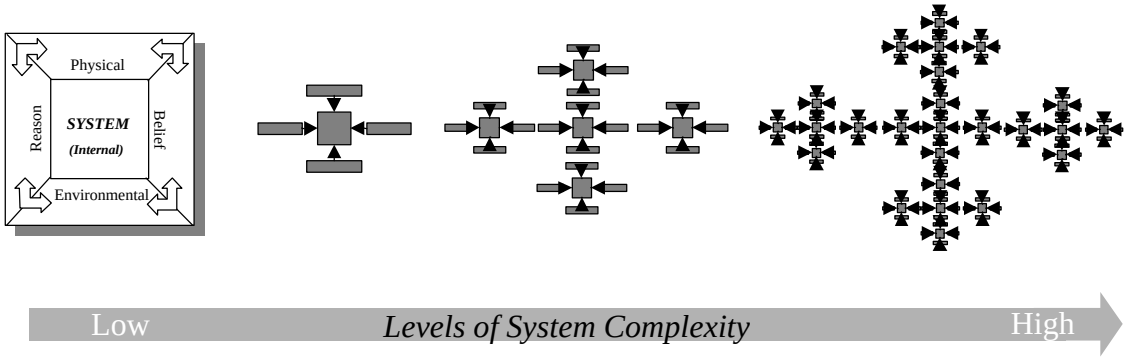
A system is a combination of basic elements or individual parts that constitute a complex, unified whole. Whereas the analytical approach ignores the interactions and focuses on the performance of the parts, the systems approach studies the linkages and relationships of the parts to gauge the performance of the system. In this context, platform-based modeling normally employs the analytical approach while effects-based modeling adopts a systems approach. The systems approach, in turn, spans a wide range of theories and tools – from classical systems theory, which uses calculus, to cellular automata, which uses adaptive agents.



In warfare, the basic "system" is composed of four sub-systems: physical, reason, belief and environmental. The physical sub-system is composed of tangible objects such as the human body, equipment, ammunition, fuel, food, weapon systems, etc. The reason sub-system includes the cognitive and neurological systems such as awareness, analysis, decision-making, and communication

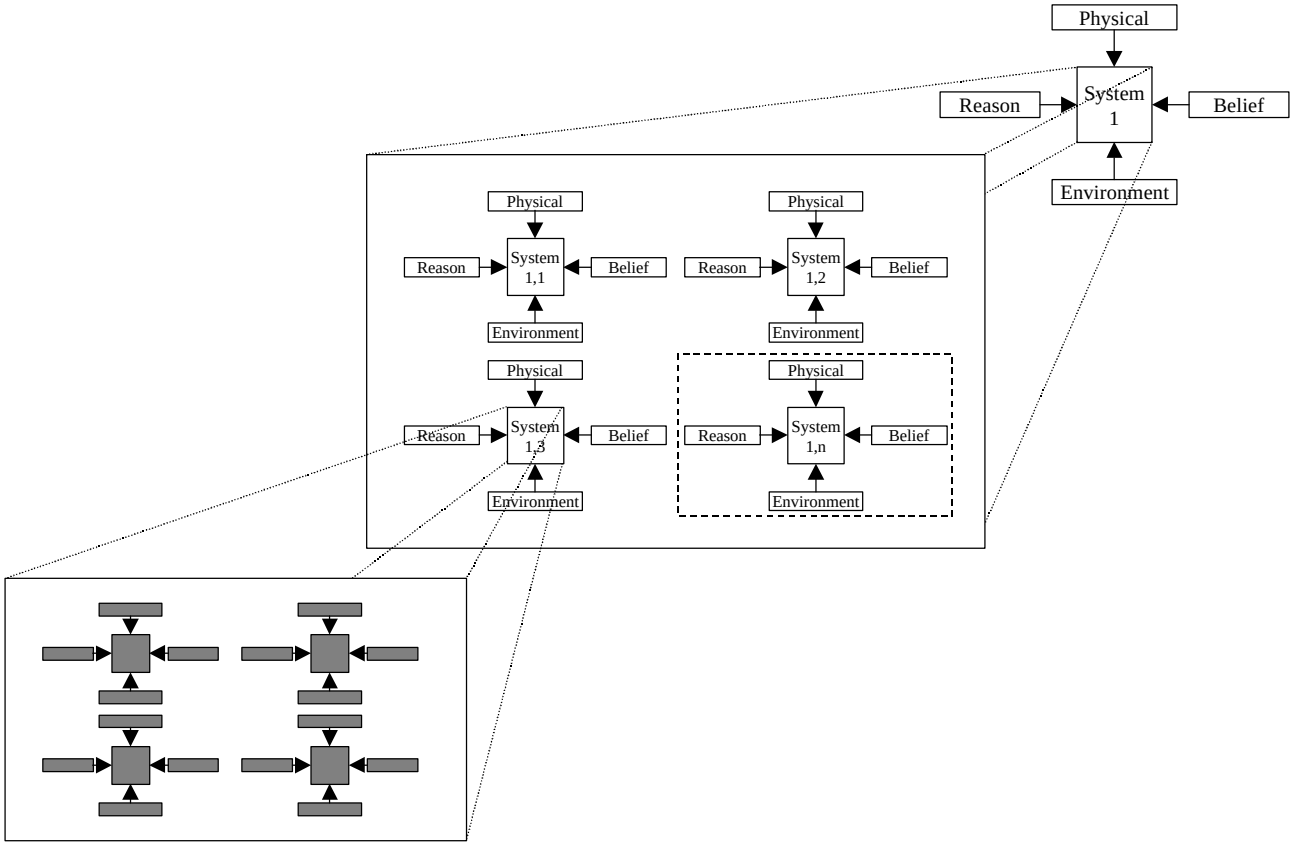
capabilities. The belief sub-system includes such things as will, leadership, cohesion, morale, fear, courage, and all human emotional and behavioral factors. The environmental sub-system includes the weather, terrain, and temporal conditions (night/day). Within the system, each of these sub-systems interact with each other, affecting the relative performance of the other sub-systems.

4..2 Recursive Systems.



A critical aspect of modeling system behavior depends on the coarse graining of the system – the level of detail necessary to describe a particular system. For example, when viewed as a series of concentric circles, the domains of physical, reason, and belief can represent different levels of modeling fidelity. Most force-on-force models measure the physical effects of the battle. Some force-on-force models and emerging information warfare models can capture aspects of the reason domain. Only a few models used for advanced research come close to modeling the affects of human behavior in the context of physical and reason activities. However, as the fidelity of coarse graining increases, so does the overall complexity of the system being described, resulting in thousands of variables and millions of potential interactions.

The goal of developing a model for Network-Centric Warfare is to strike a balance between coarse graining and technical feasibility while capturing the effects of war on the physical, reason, and belief domains. At some point a level of aggregation must be accepted in order to create a practical, working model of combat. The use of entropy measures, which capture both micro- and macro-states through statistics, offers a balance between too little and too much detail.



ii. Entropy-Based Modeling.

The Entropy-Based Warfare Model™[15] is based on the paradigm that "warfare can be directed against the cohesion of enemy units or states rather than exclusively against the physical components that comprise those entities."[16] The measure of disorder of the system, not the tally of individual elements destroyed, is the goal of the Entropy-Based Warfare Model™. To this end, the emphasis shifts from force to other factors such as cohesion, friction, and belief factors. The model calculates combat effectiveness as the result of dynamic interactions of physical energy and matter, information, and environmental conditions upon a system. The three areas of Entropy-Based Warfare correspond roughly with the three spheres of warfare:

- Physical inputs (e.g., firepower, logistics, manpower) corresponds to the physical sphere of warfare.
- Reason inputs (e.g., information, command and control execution) correspond to the mental sphere of warfare.
- Belief inputs (e.g., morale, leadership, and cohesion) correspond to the moral sphere of warfare.

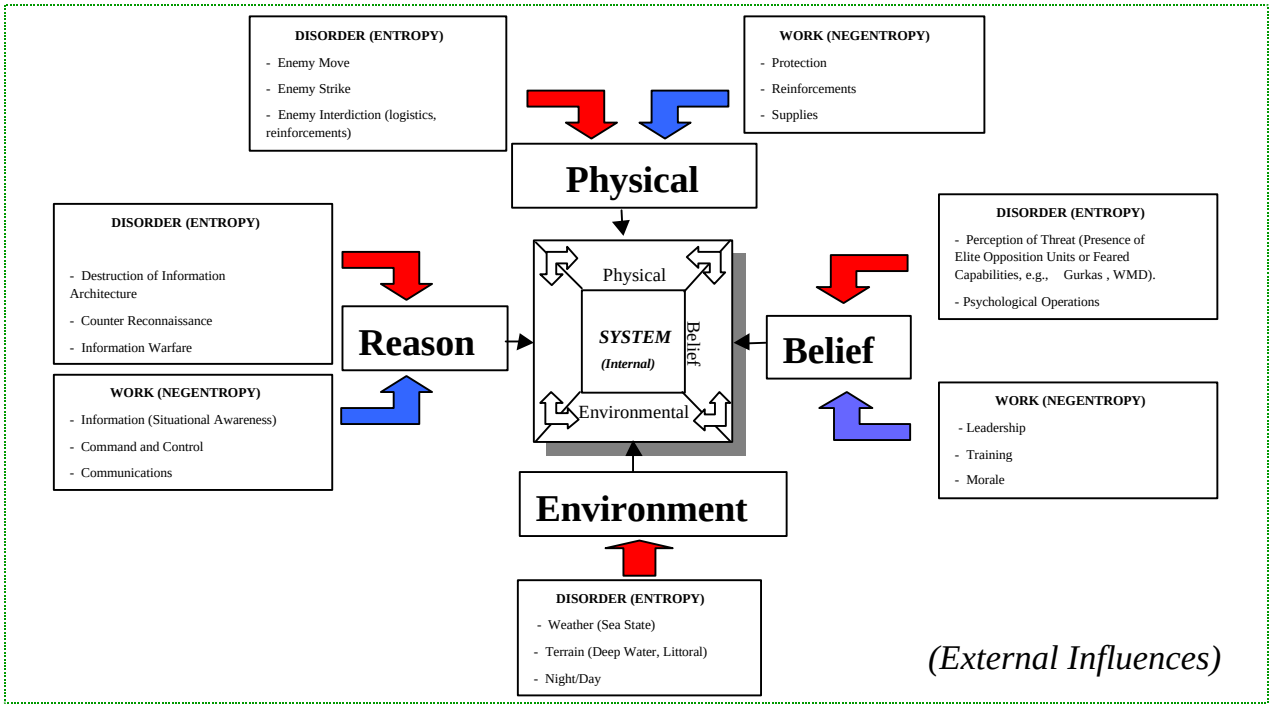
---

[15] The Entropy-Based Warfare Model™ was originally developed for the Office of the Secretary of Defense, Office of Net Assessment. The model's purpose is to take extant understanding of the Revolution in Military Affairs (RMA) and build a manual boardgame which allows players to manipulate high sensitivity variables such as space and time to explore RMA organizational and operational concepts. It was initially embodied in a manual simulation (Boardgame) but has since been automated. The automated version has since supported each service's Title X Wargame Series.

[16] Mark Herman, *Entropy Based Warfare: A Unified Theory for Modeling the Revolution in Military Affairs*, white paper, Booz •Allen and Hamilton, 1997, pp 2-3.

- Additionally, environmental inputs represent the natural environment in which the battlespace exists.

The entropy of a system consists of two inputs: internal and external entropy. Overall system performance is an outcome of the interaction of these two inputs. Internal entropy equates to the system description. It includes physical, belief, reason, and environmental elements. Internal entropy, however, is treated as an isolated or closed system. As such internal entropy remains constant or increases, the rate of which is contingent on the performance of each of the internal elements. External entropy is composed of the same elements of physical, belief, reason, and environment but unlike the internal component, the external inputs can be either negative or positive. That is, work (negentropy) can be applied to the system (negentropy) through physical (supplies), reason (C2), and belief (leadership) factors to reduce entropy. On the other hand, damage (entropy) can be applied to the system through physical (firepower), reason (C2 warfare), and belief (psychological operations) to increase entropy. Environmental factors are either neutral (benign weather) or work to increase disorder (high sea states). The environment can only be adapted to in order to mitigate against the deleterious effects. Adapting to the environment might increase *capabilities* against the enemy but it will never increase overall order. The recursive relationship between the system and the sub-system leads to a ripple effect in entropy because entropy in a system remains constant or increases. The continuous increase in one sub-system's entropy causes a corresponding increase in entropy to surrounding or higher systems. Over a period of time, continual increases in entropy leads to various phase state changes across the entire system (e.g., water to steam). The phase state change is the ultimate measure of system cohesion and is critical to capturing system collapse.



This model is binary in the sense that physical energy and mental execution can be infused to decrease overall system entropy while at the same time the adversary is trying to increase entropy through physical attacks and information warfare. Thus, warfare can be seen as a duel between competing systems working to maintain their own order while increasing the disorder of the enemy. The side that minimizes its own entropy, mitigates the effects of environmental friction, and increases the entropy of its enemy over the shortest period of time, will prove more successful.

ii. Example.

The goal of the Entropy-Based Warfare Model™ is to measure the level of disorder, especially the phase transition lines where a system moves from ordered to fluid to disordered. For example, as combat units move from garrison, where there is normally a high state of order, to contact with the enemy, the level of disorder increases at a somewhat linear pace. The amount of matter, energy, and information needed to maintain order during this transition phase is normally small because the system entropy is increasing at marginal rates. However, once contact with the enemy is made, the system reaches a bifurcation point and the level of disorder increases non-linearly, pushing both friendly and adversary forces into a state of fluidity. In order to maintain some level of acceptable order, matter, energy, and information must be injected into the system. Meanwhile, each side is attempting to disrupt the other's system by physically or mentally disrupting the other through physical or information warfare attacks. The side which can more rapidly launch synchronized physical and information attacks, while maintaining an accurate and robust feedback loop, can "self-optimize" and drive the enemy system into state of chronic disorder. The ability of a system to efficiently use energy and matter through better information processes to adapt and evolve is the hallmark of a complex adaptive system.

ii. Conclusion.

Network-Centric Warfare implies that war should be viewed as a complex adaptive system. It is complex in that it is composed of non-linear interaction of many variables. It is adaptive in the sense that the agents use feedback mechanisms to adapt to and exploit their environment. It is a system composed of hundreds of systems, sub-systems, sub-sub-systems, etc., that strive to operate as a whole in unison. In order to capture the improvements suggested by Network-Centric Warfare, the modeling paradigm needs to shift from focusing on discrete physical events to capturing larger system effects. While physical measures still matter, it is unlikely that the physical measures alone will be sufficient to capture the cognitive and behavioral aspects of warfare. A model which incorporates the complex inter-workings of physical, reason, and belief forces within a rapidly changing ecosystem will need to be developed. An entropy-based model analogous to the field of non-equilibrium thermodynamics appears to offer a better description of complex adaptive systems than classical physics-based force-on-force models.

CHAPTER 5 OPERATIONAL EXAMPLE

"You know, I am not sure that not numbers or strength bring victory in war, but whichever army goes into battle stronger in soul, their enemies generally cannot withstand them."

Xenophon, Fourth Century B.C. Greek Military Leader

ii. Introduction.

While Network-Centric Warfare will have far reaching impacts throughout multiple military operations, this analysis seeks to identify a single operational example which will illustrate the dramatic role of network centric technology and operational concepts. The end-to-end story of the operational mission will identify the specific NCW metrics which influence the overall mission within each of its discreet phases. The current doctrine and the evolving concepts identify an amphibious assault as a mission which NCW will readily complement and support from beginning to end.

As stated in Joint Publication 3-02, Joint Doctrine for Amphibious Operations, "the amphibious operation exploits the element of surprise and capitalizes on enemy weaknesses by projecting and applying combat power at the most advantageous location and time." An amphibious assault requires mobility and flexibility to accomplish the amphibious task force (ATF) final objectives. The assault incorporates forces of multiple services. Integrating these forces requires a concentration of a balanced force structure which strikes with great strength at a selected point in the hostile defense system. Within the hostile territory there are potentially more targets than means to attack them. Thus the traditional scheme of attack establishes a logical sequence that will attain cumulative results in increasingly favorable conditions.[17] Network-Centric Warfare has the potential to enable mass simultaneous attacks against multiple discreet points within the enemy defense system.

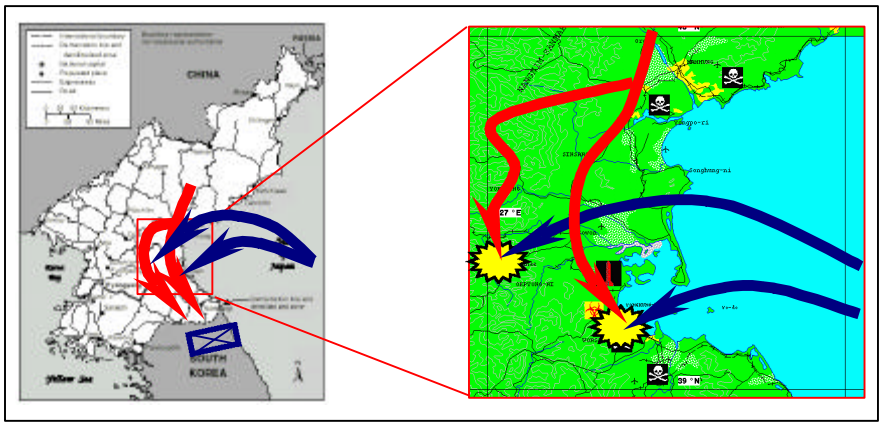
In addition to Network-Centric Warfare, the Department of the Navy is developing Operational Maneuver from the Sea (OMFTS), which advocates utilizing the sea as a means of gaining a relative advantage within the amphibious assault. The advantage stems from sea-based logistics, sea-based fire support and the use of the sea as a medium for tactical and operational movement. The integration of precision long-range weapons, greater reliance on sea-based fire support, and improved logistics of the landing force will allow a fluid and rapid transition from ship-to-shore movement to "subsequent operations ashore" without the traditional "build up phase." The rapid and dynamic tempo enabled by Operational Maneuvers from the Sea will allow US forces to act so quickly that the enemy will fail to react effectively until it is too late.[18] A Network Centric structure complements the OMFTS concept by allowing all US forces within the theater, in addition to naval forces, to support the landing force units via precision engagement, logistical off-loading, and enhanced battlespace awareness.

The following amphibious assault scenario should serve as an illustration of employing the technology and operational concepts of Network Centric Warfare.

ii. Scenario Overview.

[17] Joint Pub 3-02: "Joint Doctrine for Amphibious Operations", 8 October, 1992, sections I – VI.
[18] Ibid.

On 24 December, 2003 North Korean ground, air, and naval forces launched an integrated attack against South Korea with the intent of taking Seoul and forcing the unification of the Korean peninsula under Kim Jong Il and the Korean Workers Party. The initial assault was successful in forcing the combined US and ROK forces to draw back just outside of Seoul. After 3 days, the ROK armies and US Forces Korea, consisting of the 8th US Army, US Air Forces Korea, and US Naval Forces Korea, succeeded in halting North Korea's advance and began to attrit the DPRK's second echelon forces. Following the halt phase of the conflict, Allied forces continued to attack the North's ground forces, air defenses, and airbases, until the o defend itself had been severely degraded. After several months, US reinforcements became sufficient to stage a counter attack to push the enemy forces back across the DMZ and permanently disable North Korea's offensive capability. A critical element within this counter attack is an amphibious invasion with the intent of destroying the LOCs along the eastern transportation corridor and halting rear echelon DPRK armor forces approaching the FLOT.



The amphibious assault mission will consist of five phases within Pre-Assault and Assault stages of the operation.

I. Pre-Assault stage of the operation:

1) Destruction of Enemy Defenses Ashore
2) Preparation of Sea and Beach Area
3) Isolation of Anticipated Engagement Areas and Local Air Superiority

II. Assault stage of the operation:

4) Ship-to-Objective Maneuver (STOM) and Air Assault Landings
5) Call For Fire/Close Air Support to Assault

ii. Blue assets within the AOR.

Naval:

- 2 CVBGs, each with:
  - 1Aircraft Carrier
  - 2Cruiser w/Aegis
  - 2Destroyers w/Aegis
  - 2 Submarines
- 3+ Air Wings
  - 13 squadrons (fighters and bombers)

Landing Force:

- Marine Expeditionary Force
  - 1 Marine Division
  - 1 Marine Aircraft Wing
  - Service Support Group

Ground:

- 2nd Infantry Division
  - 2 Maneuver Brigades

        - 2 M1A1 Abrams tank battalions
        - 2 Mechanized Infantry battalions (Bradley)
        - 2 air assault infantry battalions
    - Aviation Brigade
    - Division Artillery
    - Engineer Brigade
    - Division Support Command
- 10th Mountain Division
- 1st Battalion 43rd Air Defense Artillery (Patriot) Battalion (EAAD)
- 17th Aviation Brigade

Theater ISR assets
- 4 U-2
- 4 JSTARS
- 4 AWACS
- 4 Global Hawk

ii. Red Forces within AOR.

- 2 Infantry Corps
- 3 Mechanized Corps Moving towards DMZ
- Missile Defense
    - Integrated Air Defense (IAD)
    - Artillery Rockets
    - Theater Ballistic Missiles (TBM)
    - Anti Ship Missiles (ASM)
- Air
    - Helicopter
    - Fixed Wing (Air-to-Air, Air-to-Ground)
- Naval
    - Frigates
    - Corvettes
    - Coastal Patrol Boats
    - Submarines

ii. Phase I: Destruction of Enemy defenses ashore.

KEY METRICS
Dispersion
Convergence
Concentration
Impedance
Variegation
Force Protection
Information Commonality
Dispersed Operations

An information grid created by the network centric system served to free elements within the carrier battlegroup from reliance on any single source of targeting and ISR data. Thus, the approaching force structure was able to remain dispersed to minimize the DPRK coastal patrols' ability to detect and classify the approaching Amphibious Task Force (ATF) until the attack began. While the fleet was still hundreds of nautical miles from the western coast of North Korea, combined naval and ground forces began the destruction of the coastal and likely aerial landing area defensive zones. These targets included gun emplacements, control and observation posts, anti-ship missile launchers, integrated air defenses assets, and other installations that could have been used by the enemy in opposing the assault landings. Although the less stealthy naval forces remained outside of the surface search range of their organic ISR assets, the network-centric system provided the common relevant operational picture enabled the approaching ATF to capitalize on the sensor grid, populated by the national, airborne, sub-surface and ground intelligence assets in theater. The engagement grid consisted of naval

surface fire support (Tomahawks and Extended Range Guided Munitions - ERGMs), naval air strikes, and US ground force artillery which collectively attacked the enemy facilities. The dispersed Allied shooters forced the DPRK army simultaneously to face two discreet engagement areas: the Sea of Japan and blue ground forces in South Korea. The DPRK's ability to conduct an effective counterattack against the forces in the Sea of Japan is limited given the considerable distance, stealth, and dispersion of US naval forces, as well as the DPRK's limited ability to conduct accurate long-range fires. This handicap is especially glaring against naval forces due to the North's lack of the technology to build a sensor-to-shooter system. The rapid, precise and undetected attack by the US naval forces' ERGMs and Tomahawks eliminated much of the enemy's targeting capabilities, which sufficiently impeded the DPRK forces from successfully engaging the Allied ground forces.

ii. Phase II: Preparation of Sea and Beach Area.

KEY METRICS
Variegation
Information Commonality
Speed of Command
Spatial Propagation
Self-synchronization
Massed Effects
Asymmetric Attack

Over the course of Phase I, DPRK forward observer units were able to move into position to provide sufficient target information for DPRK artillery to attempt attacking units within the US forces preparing to launch the land aspect of the counterattack. However, information provided by the MTI sensors on-board the JSTARS identified the DPRK units' movement into a position to potentially engage Allied ground forces. Before they forces could inflict enough damage to disrupt the preparation of the avenues of attack, both US ground and naval forces observed the shift in enemy's posture via the network information grid. The heightened battlespace awareness enabled both naval and ground commanders to independently target the enemy ground maneuver units. As each commander made known their independent intention to engage, the naval commander was able to immediately synchronize his actions with the ground commander over the information grid. While the ground commander engaged the DPRK artillery units, the advanced forces of the ATF continued to maneuver towards shore to begin the mine-clearing mission. Concurrently SEAL teams began destroying, removing and/or marking obstacles in the sea approaches to and on the selected beaches between the 20 foot curve of the landing area. The SEAL teams also served as additional intelligence assets contributing to the sensor grid. The ATF remained dispersed to minimized detection and classification by enemy patrol boats; however, a Perry class frigate (FFG-58) was damaged by a free-floating mine. After detecting the damaged frigate a North Korean corvette within the area immediately moved to engage. Although the naval forces were dispersed, the common operating picture made available by networking the naval, ground, and national intelligence assets provided sufficient targeting data for an AEGIS cruiser to engage the corvette with harpoon missiles from over the horizon. A Global Hawk UAV orbiting within range collected a battle damage assessment (BDA) of the attack and provided a near real-time update to the operational picture which characterized the corvette as destroyed.

ii. Phase III: Isolation of landing area & local air superiority.

KEY METRICS
Self-Synchronization
Concentration
Impedance
Information Precision
Information Commonality
Information Velocity
Speed of Command
Nodal/Link Redundancy
Network Reliability

While the naval interdiction continued, one of the SEAL teams identified an air defense battery which had remained intact near the landing zone. The crippled communications of the Perry class frigate temporarily eliminated the SEAL team's communication link to the information grid; however, redundant links within the system allowed the SEAL team to communicate via a destroyer within their line-of-sight. As the SEAL team relayed near real-time targeting and BDA information to the destroyer, two squadrons of North Korean helicopters began flying towards the littoral regions. Both ground and naval forces immediately observed the incoming air threat. An Arleigh Burke class destroyer received the target data concerning the enemy helicopters simultaneously over Link-16

and launched evolved Sea Sparrows to counter them. At the same moment, a US AAA battery officer also ordered his forces to engage the incoming helicopters. Network Centric Warfare enable the two responses to conduct a synchronized attack that destroys half of the incoming helicopters immediately and causes the remaining to return to base, thus impeding red's ability to conduct an effective air response. Just as importantly, synchronization of the ground and naval forces did not cause friendly losses. This phase of the attack continued striking the remaining IAD and LOC targets.

KEY METRICS
Self-Synchronization
Weapons Responsiveness
Lock-out
Local Force Advantage
Convergence
Massed Effects
Effect Mitigation
Force Protection

ii. Phase IV: Ship-to-Objective Maneuver & Air Assault Landings.

After establishing local air superiority and isolating the anticipated engagement areas, the amphibious assault formally began as landing crafts made the ship-to-shore movement. Simultaneously V-22s and CH-46Ds aircraft began the air assault and vertical envelopment with troops. All ISR assets within the area of operations provided the commander with a heightened awareness of the overall operational picture. The targeting information from the sensor grid allowed the naval landing, and ground forces to converge their attack on the enemy's infantry and armored forces tasked with defending against the amphibious assault. The naturally limited transportation corridors, combined with the damaged and destroyed LOCs and bridges minimized maneuverability options for the DPRK ground maneuver units. This "lock-out" of options forced the DPRK forces to engage the amphibious assault within our desired engagement areas – i.e., those under the protection from off-shore or airborne offensive and defensive shooters. Although the enemy forces possess the traditional advantage of being defenders, the simultaneous attack of stand-off platforms with a common operational picture created a local force advantage for the assault forces. In an effort to overcome this temporary local force advantage, the DPRK forces launched 5 sorties of TBMs (Scuds) at the ground troops. Notified almost immediately, US Army Patriot battery officers fired several interceptors, as did the AEGIS cruiser using several Standard interceptor missiles. The self-synchronized rapid action of the field officers, and the responsiveness of the weapon systems, led to the destruction of the incoming Scuds. A completely networked ISR, Command and Control, and engagement system enabled the near-immediate response of both forces to the threat. This allowed the Allied forces to maintain their local force advantage.

ii. Phase V: Call For Fire (CFF) & Close Air Support (CAS).

During the fight for the littoral, the local force advantage was maintained by the landing forces' ability to rapidly call in precise fire support from distant naval and ground artillery, and from air support. The redundant network pathways and nodes allowed targeting and BDA information to rapidly travel between the landing and supporting forces. It should be noted that this ability must include even the most stressing cases of high network traffic and information bundles requiring large bandwidth. Because the landing forces and supporting forces shared a consistent and relevant battlefield picture, it ensured that the CFF and CAS support would occur within the desired space and time. Thus a network centric system connecting a sensor grid with the command and control information grid will enable the engagement grid to mass strikes against enemy forces to create disorder, confusion, and eventually crippling the unit's effectiveness.

However, without accurate situational awareness, the common operational picture shared by the landing and supporting forces could become "blurred" like two identical

Speed of Command
Asymmetric Force Advantage
Convergence
Information Precision
Information Commonality
Information Velocity

transparencies overlaid slightly out of place. Using a different version of this scenario, a more aggressive DPRK would have the potential to deny the US accurate SA. Among the possible capabilities are WMD/EMP bursts, IO/IW, and sea mines that can stop US commanders from attaining minimum essential information at the critical time.

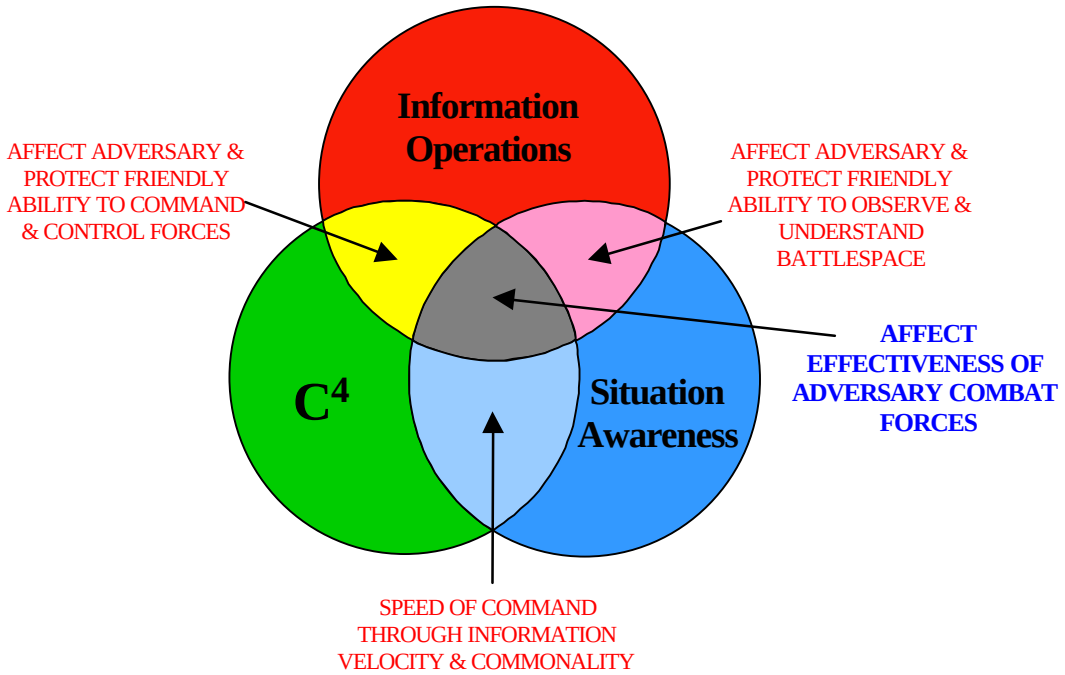
CHAPTER 6 REASON METRICS

> *"This difficulty in seeing things correctly, which is one of the greatest sources of friction in war, makes things appear quite different from what was expected."*
>
> Carl von Clausewitz, *On War*

ii. Introduction.

The metrics discussion is a critical component of this paper. At this point in the development of the metrics, only the reason and physical spheres will be analyzed in detail. The description of each metric will include a paragraph describing the key attributes of each metric. The second paragraph will put the particular metric into the context of the Operational Example set forth in the previous chapter. The metric will be discussed with regard to the particular phase of the operation, and the notional results of Blue and Red's actions.

Reason metrics are the realm of human cognition. They include awareness, analysis, and decision-making capabilities. Reason metrics measure the ability to grasp complex battlefield situations (situational awareness) and to make decisions and act upon them (C^4). Before the collection, processing, and dissemination of information became automated, the contributions of human cognition was difficult to quantify. Instead, analysis of human reason tended to concentrate on specific leaders and tactics. The emphasis was on qualitative rather than quantitative factors. To date, most of the analysis on the Information RMA concerns the study of modern C^4I systems and decision-making (i.e., the mental) and their operational impact on the weapons systems (i.e., the physical sphere). As the emphasis has shifted from individual leadership styles to network architectures and performance metrics, it has become possible



to quantify the impact of mental processes on combat power. The reason metrics include awareness, analysis, and decision-making capabilities.

The goal of this chapter is to identify key Network-Centric measures which evaluate human cognition and decision-making. It is not intended to identify measures for areas outside the realm of a network environment, such as all the elements of Information Operations (including Civil and Public Affairs). Rather, these reason metrics isolate network processes that affect the commander's (and the adversary commander's) decisions, ability to reason and make decisions, and confidence in decisions made by measuring what information is available and when. The reason sphere is the domain of information. It is centered on the ability to collect, process, use, interpret, disseminate, and act upon varying degrees of information within a network environment.

In warfare, the reason metrics are divided into three operational areas. These are Situation Awareness (SA), Command, Control, Communications and Computers (C^4), and Information Operations (IO). This cognitive area is described in Joint Vision 2010 as information superiority.

6..1 Situation Awareness (SA).

With respect to Network-Centric Warfare, Situation Awareness is defined as the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status and location in the near future. It represents the full complement of information a commander has regarding both friendly and enemy forces at critical decision points. It does not imply that a commander knows everything he needs to know about the battlespace, rather that he feels that he has enough information to be able to gain or maintain his own initiative, or negate that of the enemy. SA frames the state of knowledge available to a commander at any given point in time, and whether or not it meets their minimum level of required information.

For Network-Centric Warfare, SA answers the following key questions for a commander for a specific reference point in time and space:

- Who – Number of units, unit designation, unit performance history, identity of commander, command structure.
- What – Status, readiness, and capability of units.
- Where – Location of friendly and enemy units, supply lines and key logistics nodes, direction of approach.
- When – All related time data concerning timelines or upcoming operations
- How – Doctrine, method of advance.
- Why – Intent.

6..2 Command, Control, Communications and Computers (C^4).

C^4 is defined as the "integrated systems of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communications designed to support a commander's exercise of command and control across the range of military operations"[19]. For Network-Centric Warfare, C4 areas focus on the information processing and dissemination capability of distributed networks. This forms the information back-plane for exerting command and control. Communications and computers are resources that enable the function of command and control. For Network-Centric Warfare, the reason sphere measures the value of interconnecting disparate networks into an enterprise environment. What is the value of increased information velocity and commonality within an enterprise network in terms of a commander's reasoning and decision-making ability? Is a revolution in command and control possible?

[19] Joint Publication 1-02, DoD Dictionary, p. 109.

6..3 Information Operations.

Information operations (IO) involve actions taken to affect an adversary's information and information systems while defending one's own information and information systems.[20] Offensive IO, or Information Warfare (IW), affects an adversary's decision-makers and their ability to process and analyze information. IW is a broad class of activities aimed at leveraging data, information, and knowledge in support of military goals. IW also encompasses actions taken to adversely affect an adversary's information, information-based processes, information systems and computer-based networks. Specifically, IW targets enemy observations, ability to exercise C^2, force effectiveness, sustainment and support operations, and civil and information infrastructure. Information Warfare includes any action to deny, exploit, corrupt, or destroy the enemy's information and its functions.[21] IW views information itself as a separate realm, potent weapon, and lucrative target.

Defensive IO, or Information Assurance (IA), protects and defends friendly information and information systems. For Network-Centric Warfare, IA focuses primarily on protecting the network (nodes, links, systems) itself. Information Assurance includes OPSEC, physical security, counter-deception, counterintelligence, EW, and computer network defense. Protecting the network and information systems is absolutely critical to the continued success of NCW, and will be evaluated as a measure of robustness. These measures are common to both C^4 and Information Assurance, and are included in the C^4 section below.

REASON METRICS

SA	***C^4***	***IW***
• Effectiveness ❑ Information Integrity ❑ Information Precision • Robustness ❑ ISR Coverage ❑ ISR Redundancy • Efficiency ❑ Information Timeliness	• Effectiveness ❑ Information Accessibility ❑ Information Commonality ❑ Lock-Out • Robustness ❑ Nodal Redundancy ❑ Link Redundancy • Efficiency ❑ Information Velocity ❑ Network Reliability	• Effectiveness ❑ Synchronization of Physical and Mental Effects

ii. Situation Awareness.

6..1 Effectiveness.

Effectiveness quantitatively captures the intended or expected results of systems or operational improvements. Specifically, SA effectiveness quantifies improvements in the

[20] Joint Chiefs of Staff Publication 3-13, Joint Doctrine for Information Operations, pp. vii - viii
[21] Ibid.

ability to observe events within a situation or context. This is the Observe and Orient portion of the OODA loop. In terms of the red threat, it is the ability to locate, identify, and classify entities on the battlefield and place them within an estimation of enemy intent. For the blue data, it is the ability to discriminate between friend and foe and to understand the tactical position and situation of friendly forces which forms the essence of Situation Awareness. Situation Awareness provides the red threat and blue position data required to support operational decision-making. That is, the ability to gain knowledge of where the enemy is and where the friendly forces are in order to enhance awareness and judgement. For Network-Centric Warfare, effective SA ultimately provides a timely, accurate and consistent view of the battlespace that can be shared throughout the deployed force.

Information Integrity. Information Integrity is a function of information accuracy, completeness and consistency. It allows for providing a common view of the battlespace to operational and tactical echelons simultaneously. If we can provide accurate, minimum essential information regarding blue and red forces simultaneously to all echelons of command, then we can coordinate attacks between multiple units, resulting in higher probabilities of correct, or desired, joint execution.

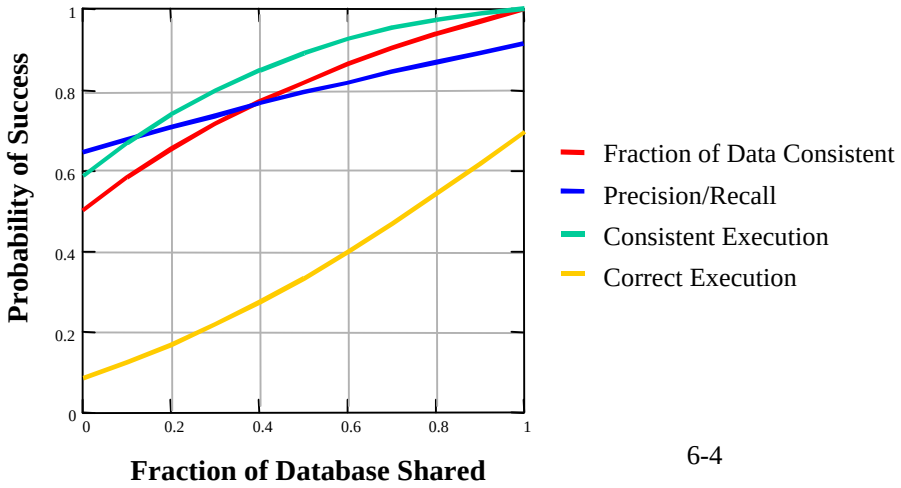
- *Accuracy* is the ability to provide information that is free from error. It is characterized by the percentage of targets within a database that are current and classified correctly. This will be especially critical as enemy Information Operations capabilities, as well as friendly vulnerabilities, continue to grow.

- *Completeness* is the ability to provide all critical information needed to accomplish the task. It is characterized by the percentage of all targets who are current and classified correctly. This aspect of the metric comes with a warning: we will never know what we don't know, or can't see, but will have make decisions and take action with some level of minimum essential information. It must be noted that even 98% information completeness may not be sufficient if data pertaining to WMD is not captured by that.

- *Consistency* is the ability to present like information and indicators in the same manner. It is characterized by the percentage of data in the database shared with other units over time.

Together, these three characteristics describe the degree of information integrity within a network. They form the metric to measure an ability to successfully plan for coordinated attacks between multiple units. The metric is the fraction of the database shared as a function of the probability of success.

For example, the metric here is depicted in Phase III of the operational example (Ship-to-shore and air assault landings) where the Navy is coordinating activity against five incoming Scud missiles with the Army. The targets were all moving very rapidly while a combination of overhead, Navy, Air Force and Army sensors were used to track their flight. The services all received the same national data, yet shared only a fraction of their own data with their forces. The x-axis represents varying degrees of shared database consistency while the y-axis represents the probability of success.



Database accuracy equals the percentage of database queries that result in current, accurate data. Database completeness equals the percentage of targets that have a current entry in the database. The probability that all units have the same view of all of the targets is calculated, along with the probability that all units have a current and correct view of all of the targets.

In this metric example, the fraction of data consistent is at 50% without inter-service sharing of information. However, Inter-service sharing raises target awareness (Precision/Recall) from 62% to 90%. Consistent execution requires the two Services to have consistent data on all of the targets. In this example, consistent execution begins at 60% and is raised to 100% by database sharing. Lastly, Correct execution requires the Services to have current and correct data on all of the targets. The probability of successful, or correct, execution is raised from 10% to 70%. This form of information sharing through Information Integrity is key to the success of NCW, especially as it will apply to joint operations.

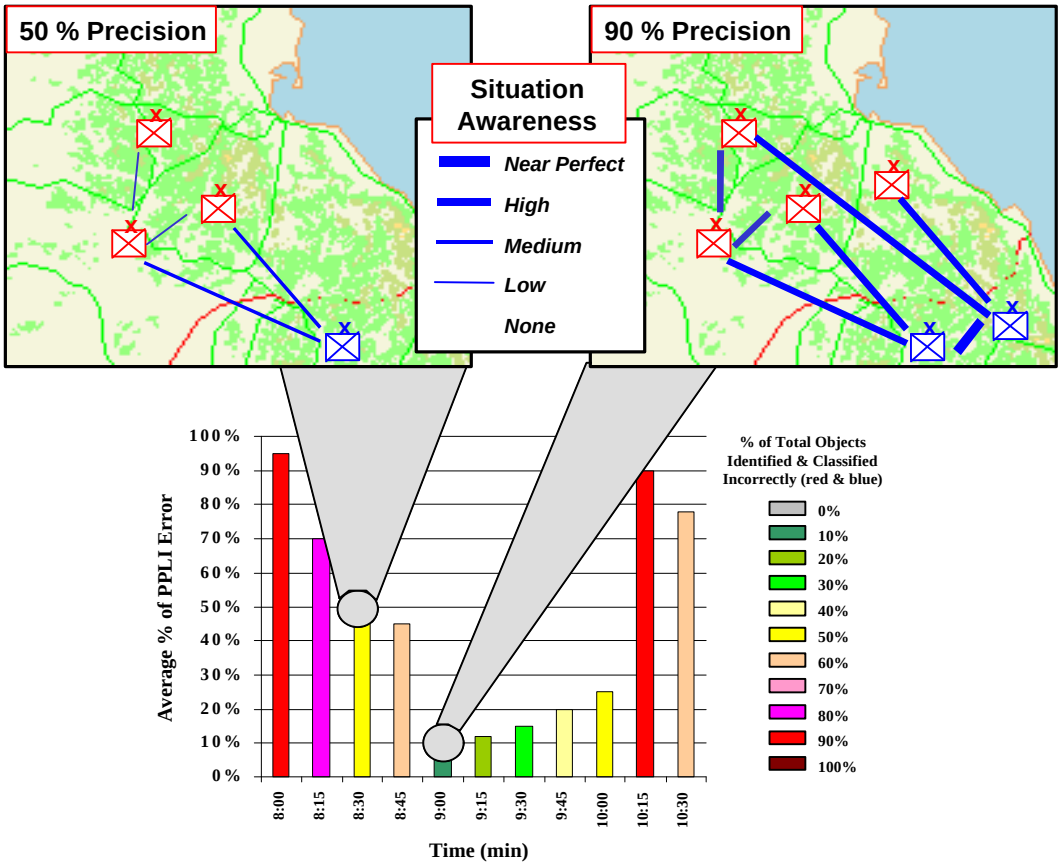
Information Precision. Information Precision is a function of fidelity. It is the degree of information refinement. Precision information is exacting and sharply defined. Precision provides the ability to distinguish an object from all other entities, determine if the object is friendly, hostile, or neutral and establish an exact location. Information Precision has three elements. These are Identification, Classification and Precise Position Location Information (PPLI).

- *Identification* is the process of assigning identities to objects and differentiating between friendly, hostile, or neutral entities. Every object has a unique identity. An identity is an attribute, or a set of attributes, that allow an object to be uniquely specified and distinguished from other objects. Identity attributes discriminate between, but do not classify, objects. For example, object attributes may be "tires", or "tracks." In this case, the object would be identified as either a wheeled or tracked vehicle.

- *Classification* is the process of assigning objects to specific categories (tank, missile, truck, etc.). Classification attempts to organize identified objects based upon multiple category discriminators. For example, a high level classification may be a truck. Lower level classifications may place this truck in tonnage categories or discriminate based upon the number of axles.

- *Precise Position Location Information (PPLI)* is the process of assigning exact latitude, longitude and elevation coordinates to an object in three dimensional space at a given moment in time. Precision is determined both in spatial and temporal terms. Precision location information is required for both friendly and enemy objects.

Together, these three Information Precision characteristics describe the optimal degree of granularity for every object in the battlespace at a given time. They form the metric to measure an ability to answer the following questions. Where am I? Where is the enemy? Where are the friendly forces? The metric is the average PPLI error and percentage of total objects identified/classified incorrectly as a function of time.



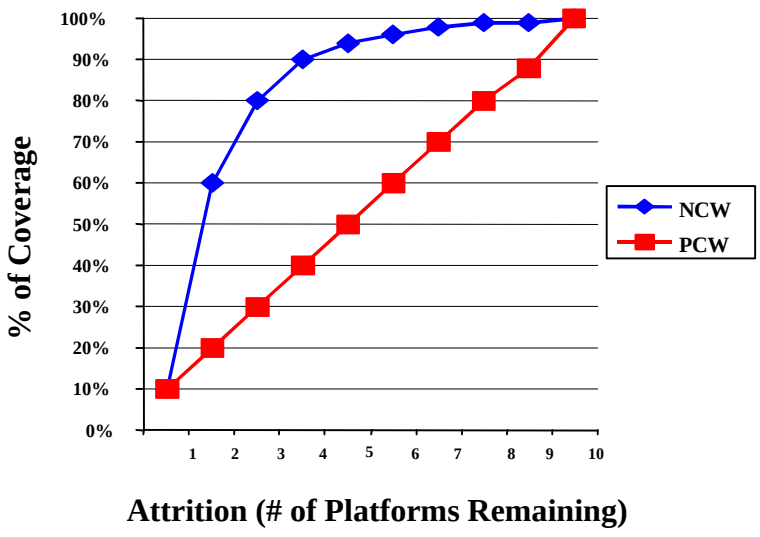
Information Precision

For example, the metric above illustrates the DPRK and US force lay-down in Korea during the final phase of the operational example. The graph represents the degree of Information Precision for both Red and Blue forces at a given point in time. The x-axis represents time in fifteen minute intervals. The y-axis measures the average PPLI error for all the objects in the battlespace. The bar colors indicate the percentage of total objects which have been incorrectly identified and classified. The combination of bar height (PPLI) and color (identification/classification) indicate the degree of precision for a given period of time. This metric is then projected as a representative example of information presented to a commander. The picture on the left represents a significantly lower degree of SA precision (50%) than the picture on the right (90%), which was used by the US commander in the example to expedite effective calls for fire and close air support versus the known DPRK ground units threatening the US forces ashore.

6..2 Robustness.

Robustness is a measure of the overall health and ability to withstand attack of a system. It implies the ability to avoid or absorb damage with minimum operational impact. Robustness is associated with depth, strength, and redundancy. Specifically, SA robustness quantifies the ability to absorb damage to intelligence, surveillance and reconnaissance (ISR) assets and still maintain adequate coverage of the battlespace. A robust SA capability maintains an ISR capability over a wide area (coverage), while at the same time insuring operational depth (redundancy).

ISR Coverage. ISR Coverage is a function of space. It is the ability to maintain an ISR capability across the breadth and depth of the battlefield. If we can network sensors to share ISR information across service and platform boundaries, then we can position ISR assets to effectively cover enemy territory, resulting in efficient sensor coverage without duplication. The placement and positioning of ISR assets determines the quantity of enemy territory covered. It is a function of ISR type and capability to hold key enemy nodes at risk to intelligence exploitation. Effective ISR Coverage will provide detection opportunities over the widest possible target array, resulting in efficient exploitation of the battlespace by those benefiting from the common operating picture. The metric is the quantity of red area covered as a function of ISR attrition.

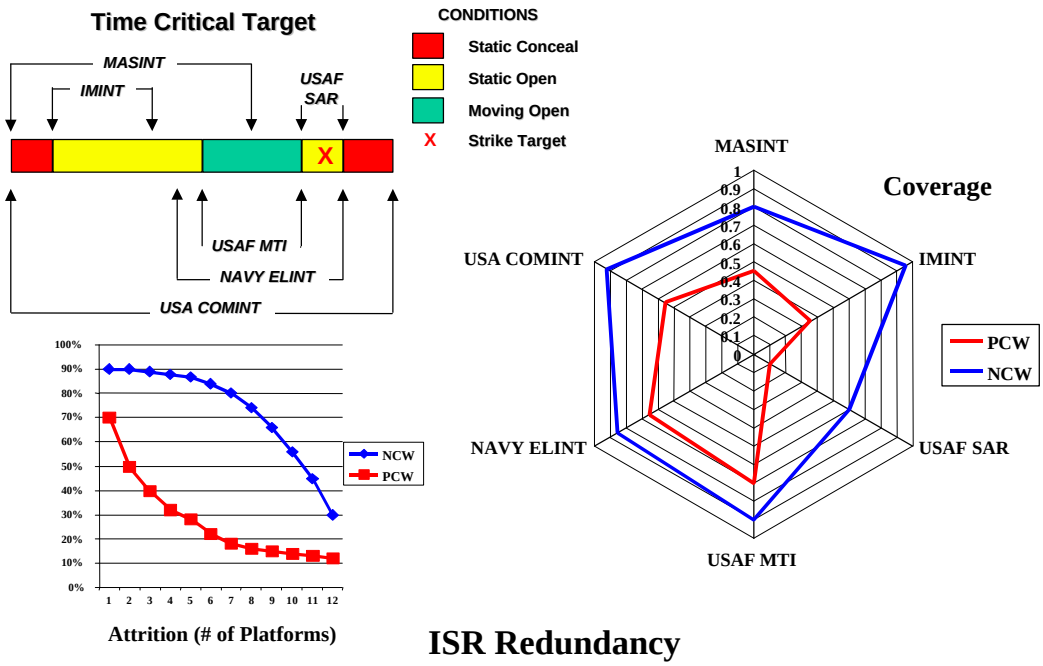


ISR Coverage

For example, the graphic above compares the relative coverage of a Platform-Centric Warfare (PCW) force with a Network-Centric Warfare (NCW) force like that described in the operational example. The x-axis represents the number of ISR platforms remaining after enemy attrition. The y-axis indicates the total percentage of area covered by the surviving ISR assets. The PCW plot is linear, since ISR information is not shared in near real-time across a common network. The NCW plot is asymmetric, maintaining a higher percentage of coverage even after suffering increased ISR attrition. The PCW ISR attrition is representative of single points of failure. The NCW ISR attrition overcomes these single points of failure by the reliability of the distributed ISR network as a whole. This discussion is more notional than the other metrics due to the DPRK's inability to attack and attrit Allied ISR platforms in any phase of the operational example, short of nuclear/EMP burst or IO against friendly systems/infrastructure supporting collection of satellite data.

ISR Redundancy.

ISR Redundancy is a function of information fusion. It is the ability to maintain Situation Awareness in the face of an enemy counter-ISR campaign. Platform-centric sensor systems utilize stovepipe dissemination pathways into individual processing and exploitation systems. If a given sensor is destroyed, then the target coverage may be lost even if another sensor is providing coverage in the area. This loss results from stovepiped, non-interoperable networks, which cannot share data in near real-time.



ISR Redundancy

ISR Redundancy off-loads data from individual sensor platforms and transfers this capability to a network. If one individual sensor, or type of sensor, is destroyed or fails, then information being fused within the network from other sensors may still provide adequate coverage. If we can share all types of ISR information from each of the collection types within one common network, then we can fuse this information into a common threat picture, resulting in increased ISR redundancy and a capability to absorb ISR attrition. The metric is the percentage of total area covered by each ISR type (COMINT, ELINT, IMINT, etc.) as a function of enemy attrition of US ISR assets.

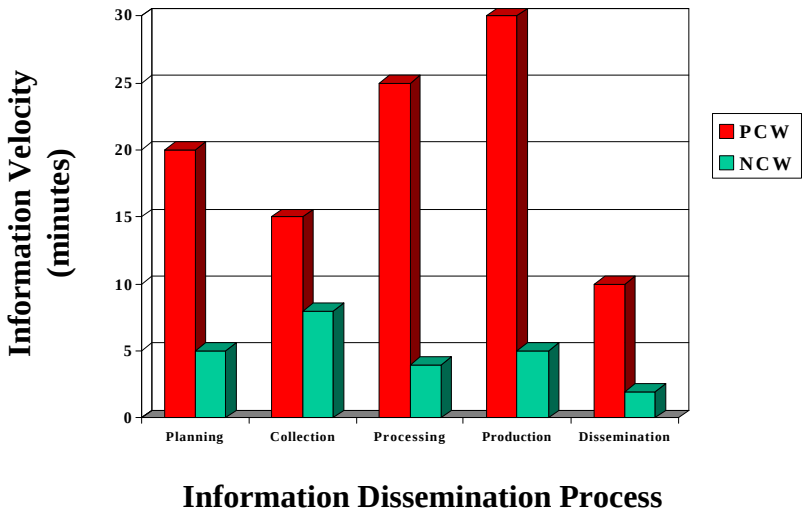
For example, the metric illustration above measures ISR redundancy for a time-critical target type. In Phase III of the operational example, the target set was a set of 5 mobile TELs, which utilized a set duty cycle, moving from a concealment site and back again. This type of target was widely distributed over the entire battlefield. Sensor coverage requirements differed at each stage of the target duty cycle, depending upon target state (moving, stationary) and location (concealed, open). Continuous coverage is dependent on the ability to correlate and fuse information from different sensor types, often from different services, across a wide geographical area. In a Platform-Centric Warfare (PCW) environment, the volume of area covered is restricted for each type of sensor, because the information is only disseminated within service stove-piped networks and is not fused across service boundaries within a common network. In a Network-Centric Warfare (NCW) environment, the percentage of total coverage is increased for each sensor type because of information fusion within a common joint network. As a result, the percentage of coverage remains high the US was able to engage the launchers.

6..3 **Efficiency**.

Efficiency is the ratio of work accomplished or energy expended relative to material inputs or time. In short, it is the accomplishment of a task with the minimum expenditure of time and effort. Specifically, Situation Awareness efficiency quantifies the time required for a commander to obtain the necessary information to maintain a high operations tempo, or prevent the enemy from doing so. In short, information timeliness drives the commander's decision cycle and can significantly alter the relative operational tempo ratio.

Information Timeliness. Information Timeliness is a function of information velocity vis-à-vis the requirement. It is the capability to process and disseminate ISR and blue position location information rapidly in order to support near real-time situation awareness. A network-centric force can fuse enemy and friendly position location information within a common distributed network, then we can increase the speed of common situation awareness, and information dissemination, resulting in near real-time intelligence across the battlespace. This will finally help to alleviate the age-old frustrations of commanders forced to delay time-critical decisions pending receipt of a single piece of information. However, decision-making timeliness will always by driven by individual commander's cognitive abilities. NCW may initially compound the problem and will require advances in data fusion, decision aids/support, and human-computer interfaces. The metric is the length of time required to complete each phase of the information dissemination process as a function of velocity.

For example, Information Timeliness may be measured using the intelligence cycle as a metric over time. The y-axis measures the intelligence cycle as a linear process. The x-axis reflects time passage in minutes. Each bar measures the time required to complete each step of the process, from planning through dissemination. A PCW environment uses a service-only, or intelligence specialty, domain network to vertically exchange information within a limited community. A NCW environment makes information exchange ubiquitous horizontally across each step in the process, dramatically increasing the velocity of information at every step in the process. In the case of the DPRK helicopter attack in Phase III, the US was able to execute each step in this process quickly enough to meet the threat with both ground (AAA) and air (Advanced Sea Sparrows) assets.



Information Timeliness

ii. Command, Control, Communications and Computers (C^4).

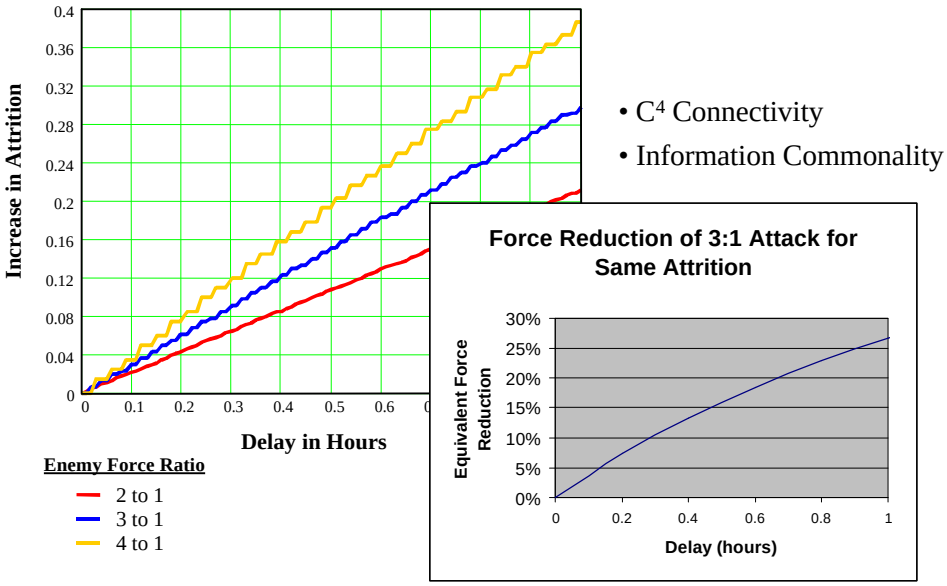
6..1 Effectiveness.

Effectiveness quantitatively captures the intended or expected results of systems or operational improvements. Specifically, C^4 effectiveness quantifies improvements in the ability to make decisions and act upon them. This is the Decide and Act portion of the OODA loop. It is the ability to access information to support cognition. That is, the ability to gain knowledge to enhance awareness and judgement. For

Network-Centric Warfare, effective C^4 provides an enterprise computing environment, where information is ubiquitous (information commonality) and accurate (information consistency).

Information Accessibility. Information Accessibility is a function of network connectivity. It is the ability to locate and retrieve information in databases, get to local or remote applications and services, and/or use work files from anywhere within an enterprise environment. Information accessibility within a Network-Centric environment enables more effective force coordination. If a force can access common information within a network simultaneously, then their execution can be coordinated in near real-time, resulting in effective use of force through simultaneous action. Effective coordination, or synchronization, is the ability to bring force to bear in the same spatial coordinate with the desired temporal sequence. Decision time is reduced through virtual coordination within the network, and actions may be synchronized in time. The metric is the time delay between Blue forces converging on an objective as a function of their attrition.

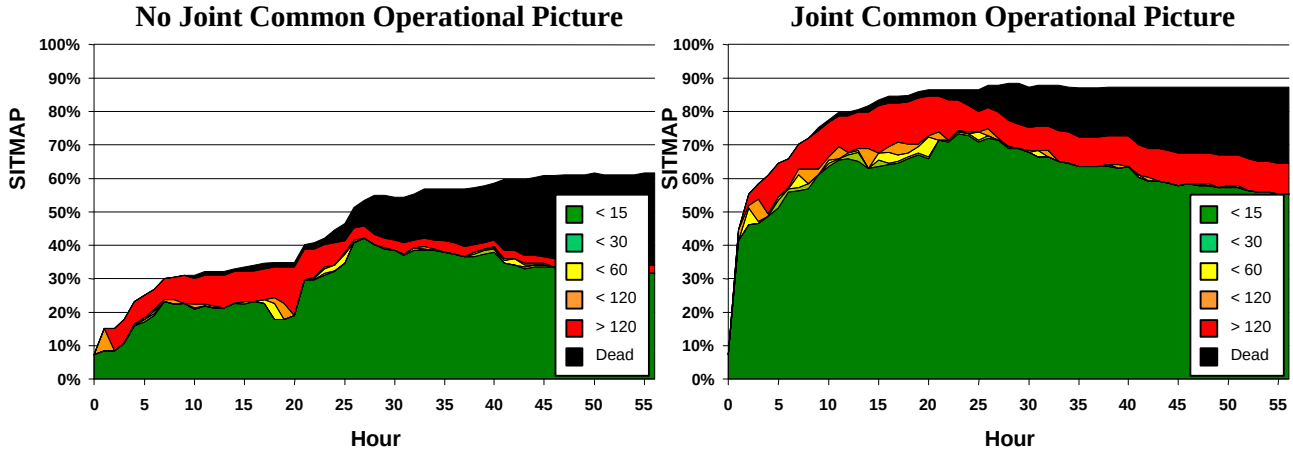
For example, the metric here depicts a scenario with two to four blue units trying to attack one red unit. Blue units arrive one at a time evenly spaced with time measured along the x-axis. The y-axis indicates increases in blue attrition caused by these arrival delays. The lack of coordination prevents synchronized arrival on the objective, effectively reducing the force ratio as a result. The force reduction graph demonstrates this principle. This graph uses a beginning force ratio of three-to-one as an example. As blue units arrive on the objective with time delays (x value), the equivalent force reduction is measured (y axis). The end result is an overall reduction in effectiveness from zero to thirty percent. This level of attrition may have occurred in Phase IV of the operational example had there been delays when the US amphibious and air assault forces landed simultaneously. Had the network connectivity been reduced, the US forces would not have enjoyed a local force advantage, and would have had suffered from delayed or degraded precision fire support. In either case, it would have led to greater Allied casualties on the ground.



- C^4 Connectivity
- Information Commonality

Information Accessibility

Information Commonality and Consistency. Information Commonality and Consistency is a function of timeliness and completeness. It is the ability to share information which possesses common features and attributes across service and platform boundaries in a timely manner. Specifically, Information Commonality refers to sharing perishable information between the services and disparate units. This time-critical information includes red threat and blue and neutral position location information, along with a common map underlay and reference data. If we can use a network to fuse red threat and blue position location information from all four services and critical ISR-providing agencies, then we can provide a common operational picture to all command echelons simultaneously, resulting in a virtual near real-time coordination, synchronization and de-confliction capability. In effect, the common operational picture resident within the network becomes a virtual control measure for dynamic battle management and command and control of joint forces. The metric is the percentage of red and/or blue and white units in the



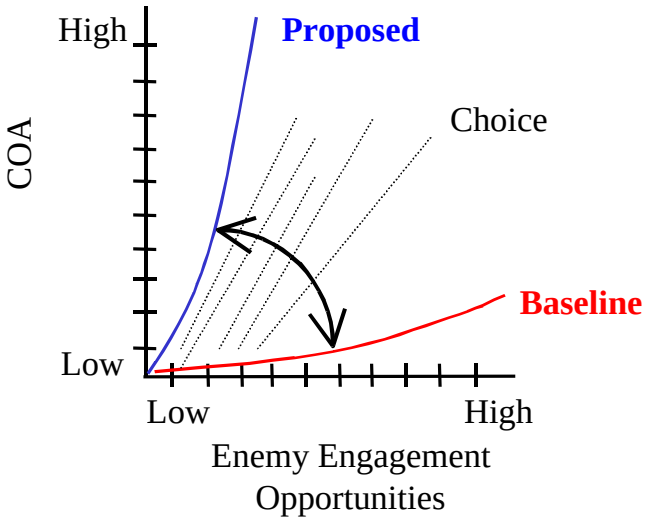
Information Commonality & Consistency

common situation map over time as a function of information latency.

The metric shown above is an example of red threat Information Commonality. The left chart displays the data for individual service pictures only (0% Information Commonality). The right chart displays the data for a common operational picture across service boundaries (100% Information Commonality). For each chart, the x-axis represents hourly time passage in a campaign. The y-axis captures the completeness percentage for red units, with 100% indicating "ground truth". The graphed shaded areas indicate the age of the information. A color coded scale indicates the appropriate latency, from 15 minutes or less up to 120 minutes and beyond. The degree of Information Commonality may be assessed through a direct comparison of these two graphs.

Lock-Out. Lock-Out limits the courses of action available to the enemy, effectively "locking out" options available. To limit the enemy's options, a force must be able to exert direct influence and power over all aspects of the battlespace: cyberspace, aerospace, land, and sea lanes of control. This can be achieved by identifying the enemy's key centers of gravity and then conducting self-synchronized strike operations to selectively limit enemy engagement opportunities. Examples of such operations include attacking the enemy's C2 nodes, critical enabling functions (transport or logistic capabilities), or key assets (i.e., maneuver units). A successful attack on these targets would result in a critical freedom of action for friendly forces. This freedom of action provides a high course of action variability, allowing friendly forces to seize and maintain the initiative. The enemy is forced to react, rather than be proactive. The enemy is presented with a "Hobson's choice", appearing to have choices when in fact there are none. For example, total airspace control over enemy territory presents the enemy with limited choices, since all known vulnerable (i.e., not deeply buried) targets may be subjected to attack from the air. A lock-out can also be achieved through effective maneuver warfare featuring the denial of key terrain through capture or control or the area and/or the denial of the area to the enemy. The metric is the number of enemy engagement opportunities as a function of blue course of action variability.

For example, the metric illustration captures the relationship between enemy engagement opportunities and courses of action available to a friendly commander. The x-axis represents the number of enemy engagement opportunities, from low to high. The y-axis measures the number of courses of action available to the friendly commander, again from low to high. The baseline represents a Platform-Centric environment, where a high number of enemy engagements severely limits the blue commanders courses of action. The proposed line represents a Network-Centric environment, where friendly course of action variance is high as a result of limiting the number of enemy engagement opportunities. The delta between the two graphed lines represents the Lock-Out phenomena, effectively limiting the enemy courses of action to a "Hobson's Choice". This dilemma is evident throughout the operational example, as the DPRK was consistently faced with only a few unappealing choices. Their primary reactions, embodied by Scud missile and attack helicopter strikes, were easily countered by a more responsive US force.

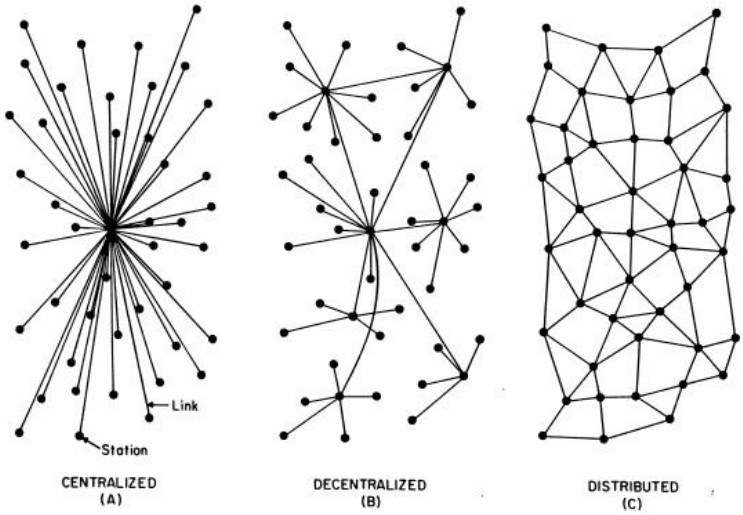


Lock-Out

6..2 Robustness.

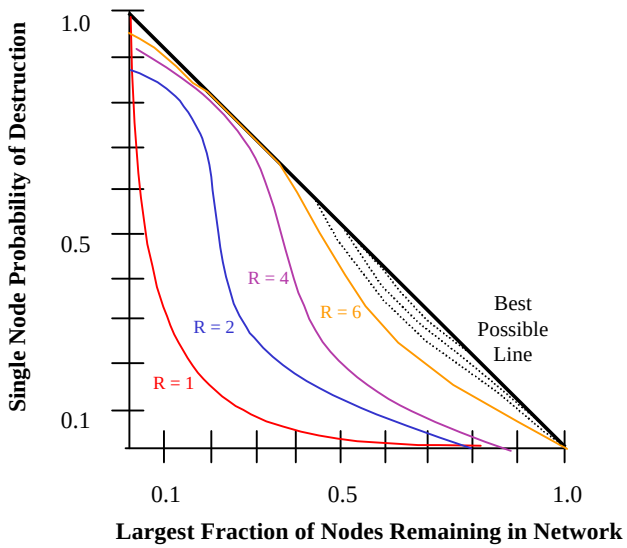
Robustness is a measure of the overall health of a system. It implies the ability to avoid or absorb damage with minimum operational impact. Robustness is associated with depth, strength, and redundancy. Specifically, C^4 robustness quantifies the ability of a network to absorb damage as a function of network distribution (survivability) and redundancy. Network survivability depends upon the number of nodes and links within a network, and upon the distribution of those nodes and links over wide areas. A robust network does not have single points of failure. Rather, a robust network maintains strength through nodal and link redundancy and geographic dispersion.

There are three basic types of networks. Networks may be centralized, decentralized, or distributed. A centralized network is routed through a single point, creating a star pattern. Centralized networks have a single point of failure, thus making it very difficult for the nodes to communicate and coordinate should they lose connectivity to the commander. Decentralized networks are a series of centralized networks linked together, forming a mesh of stars. Decentralized networks have a hierarchical structure,



relying on multiple points of failure. A distributed network is interwoven, creating a complex lattice of nodes. Decentralized networks have a link-to-node ratio equal to the square of the number of nodes. This represents a high degree of redundancy, or an exponential growth in points of failure.[22]

Nodal Redundancy. Nodal Redundancy is a function of nodal distribution within a contiguous network. It represents the number of nodes remaining functional after an adversary's attack. Surviving nodes are defined as nodes which survive the attack and maintain an ability to communicate and operate together as a coherent entity after the attack. Small groups of nodes isolated from the single largest surviving group are therefore considered to be ineffective. If a distributed network is built with a set of redundant nodes, then it can maintain a high level of nodal connectivity after an adversary's attack, resulting in a high degree of network integrity after enemy attacks. The metric is the fraction of stations remaining in communication as a function of enemy node probability of destruction.



Node Redundancy

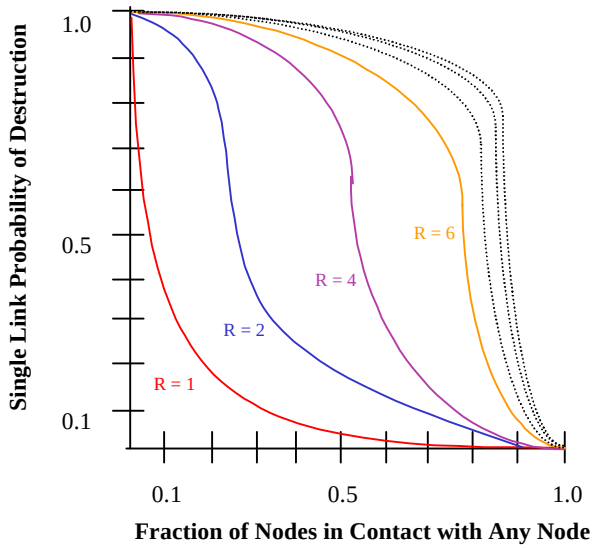
Redundancy levels are used to measure connectivity within a distributed network, as shown in the figure on the previous page.[23] A minimum network spanning three nodes is defined here as a redundancy level of one. If two times as many links are used in a network grid than in a minimum span network, the network is said to have a redundancy level of two. This process repeats itself through redundancy levels 3 through 8. The redundancy level is equivalent to the link-to-node ratio in the array of stations. The higher the redundancy level, the greater the degree of survivability. The notional metric example here represents the effect of enemy nodal targeting against a distributed network. The x axis represents the largest fraction of nodes remaining within the network. The y axis represents the single node probability of destruction by the enemy. Each line reflects a redundancy level based upon nodal connectivity within the distributed network. As redundancy levels increase, a larger fraction of nodes survive enemy targeting. Redundancy levels increase as you move to the right of the graph, ultimately reaching the best possible line (R=10).

In terms of the operational example, the amphibious and surface support forces were part of a distributed network, thereby presenting the DPRK forces with an insurmountable targeting task. This is especially true given the North Korean's inability to generate sustained simultaneous long-range precision strikes versus any identified allied nodes.

Link Redundancy. Link Redundancy is a function of multiple links, or pathways, within a distributed network. It represents the number of links remaining functional after an adversary's attack. Surviving links are defined as pathways which survive the attack and maintain an ability to connect nodes, either by direct electrical or radio frequency connections. If a distributed network of redundant links is built, then it can maintain a high level of nodal connectivity after an adversary's attack, resulting in a high degree of network integrity after enemy attacks. The metric is the fraction of nodes remaining in communication with any other node as a function of enemy link probability of destruction.

[22] RAND, Memorandum RM-3420-PR, On Distributed Communications, Introduction.
[23] RAND, Memorandum RM-3420-PR, On Distributed Communications, Introduction.

As with nodal destruction, redundancy levels are used to measure link survivability. The metric example here represents the effect of enemy link targeting against a distributed network. The x-axis represents the fraction of nodes in contact with any node. The y-axis represents the single link probability of destruction by the enemy. Each line reflects a redundancy level based upon link connectivity within a distributed network. As redundancy levels increase, a larger fraction of links survive enemy targeting. Redundancy levels increase as you move to the right of the graph, ultimately reaching the best possible line (R=10). Similar to the nodal redundancy's relationship to the operational example, the nature of the DPRK's forces and C2 structure and capability would preclude them from successfully targeting a sufficient number of Allied links to disrupt any phase of the operation.



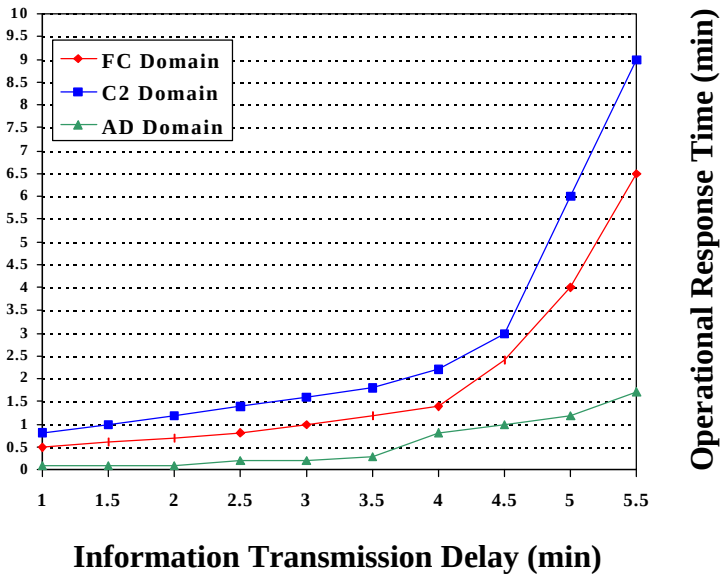
Link Redundancy

6..3 Efficiency.

Efficiency is the ratio of work accomplished or energy expended relative to material inputs or time. In short, it is the accomplishment of a task with minimum expenditure of time and effort. Specifically, C^4 efficiency quantifies improvements in speed of command. That is, the ability of a commander to give commands to subordinates and to receive feedback from those subordinates in order to exercise control. Thus, this is also a measure of how efficiently the OODA loop is being executed. Efficient C^4 relies upon high network accessibility to an enterprise computing environment to allow a NCW force to operate as efficiently as possible.

Information Velocity. Information Velocity is predominantly a function of time. It is the capability to identify the required nodes within the network and then move information from one node to another rapidly. A high information velocity will allow the network to respond in support of operational tasks in a much more timely manner than as historically been possible. Information Velocity may be degraded by nodal or link targeting, volumetric saturation, bandwidth availability or service, platform, or alliance interoperability problems. If information can be passed across a distributed network in near real-time, then the information can be exchanged in order to dynamically coordinate, de-conflict and synchronize activities, resulting in rapid operational response times. The metric is the operational response time as a function of information transmission delays within the network.

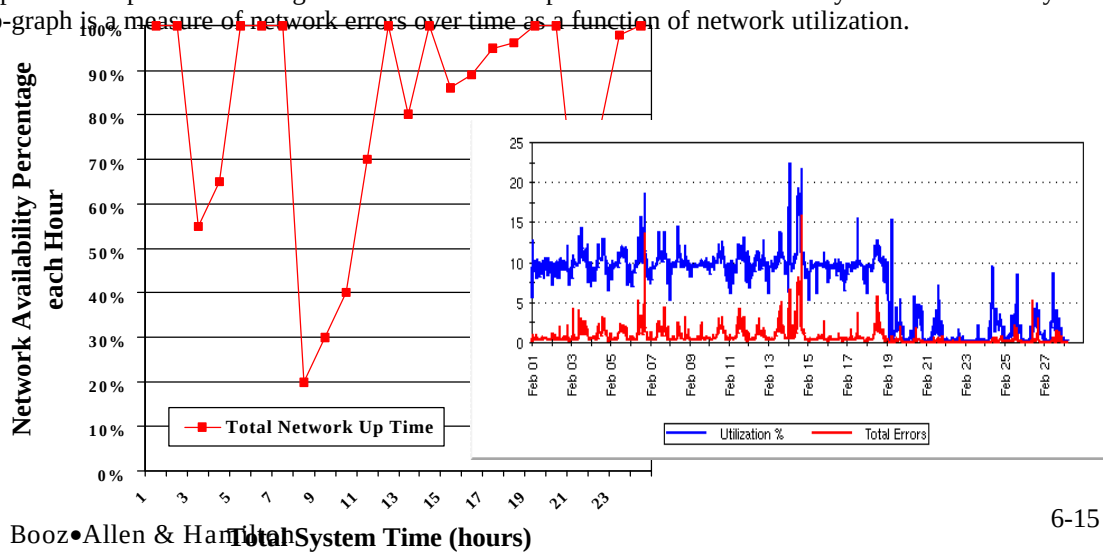
The metric illustrated on the graphic to the right represents notional operational impacts from network information delays. The x-axis measures the total transmission delay from an originating node to a destination node. The y-axis measures the corresponding operational response time delay. The graphed lines represent the operational impact of information delay on representative domains within the network. Information delays can result in non-linear operational effects. While all information delays can result in lower probabilities of hitting time critical targets, the notional chart illustrates that it is the tasks that require a decision cycle (i.e., C2) that incur the largest operational cost due to the transmission delays. Targets must be re-acquired and new information must be transmitted through the network for effective C2 and fire control. These feedback loops often cause asymmetric delays in operational responses.



Information Velocity

Network Reliability. Network Reliability measures the percentage of time the system is operational and available to the warfighter – obviously an acute requirement for a Network-Centric force. A reliable network will consistently be available for use over time and across a wide variety of circumstances. Network Reliability also measures the frequency and types of errors which cause hardware and/or software breakdowns. If a network's errors can be minimized over time, then its total effective time will be greatly increased, resulting in consistent network availability to the warfighter. The metric is the percentage of network availability over a period of time. Given the nature of the amphibious operation described in the previous chapter (e.g., dispersed forces, long-range fire support, etc.), any major degradation to the network and the common and consistent operational picture at a critical time could have disastrous effects on the Allied forces.

In the example metric on the next page, the x-axis represents one hour increments for a given day. The y-axis represents the percentage of time each hour the network was operational and available for use. The graphed line represents a histogram of total network up time as a measure of daily network efficiency. The sub-graph is a measure of network errors over time as a function of network utilization.



ii. Information Warfare.

Network-Centric Warfare is both an enabler of, and lucrative target for, Information Warfare. NCW focuses the power of the network by linking together disparate networks. It increases total combat power through inter-linking physical engagement networks with information engagement networks. This is the bridge between Network-Centric Warfare and Information Operations. The IW metric described in this section measures the synergistic effect of combining Network-Centric Warfare concepts with Information Warfare concepts. It demonstrates the value in combining the physical attack benefits from Network-Centric Warfare with the Information Attack benefits from Information Operations.

Synchronization of Physical & Mental Effects. Synchronization of Physical and Mental Effects is a function of IW attack and physical attack coordination in time. It is the ability to inter-link IW operations with maneuver and strike operations through a common network. IW operations include electronic warfare, psychological operations, and computer network attack. The resulting synergy is created through simultaneous execution of events across the physical and reason spheres of war. If a force can integrate maneuver and strike activities with IW activities through a common network environment, then they can synchronize physical and mental operations in time, resulting in significant operational impacts to an adversary's ability to command, control and execute operations. The metric is the percentage of an adversary's force affected as a function of time (duration of effect).

IW and physical attacks both target common enemy activities. These activities include an adversary's ability to conduct physical operations (e.g., move, strike, protect) and to conduct mental operations (e.g., sense, command, communicate). Both mental and physical attacks have the potential to inflict limited, moderate and significant damage on the enemy's capability to wage war. However, Network-Centric Warfare provides a means to integrate these activities into a synchronized whole. The network provides a capability to create effects which are greater than the sum of the individual parts.

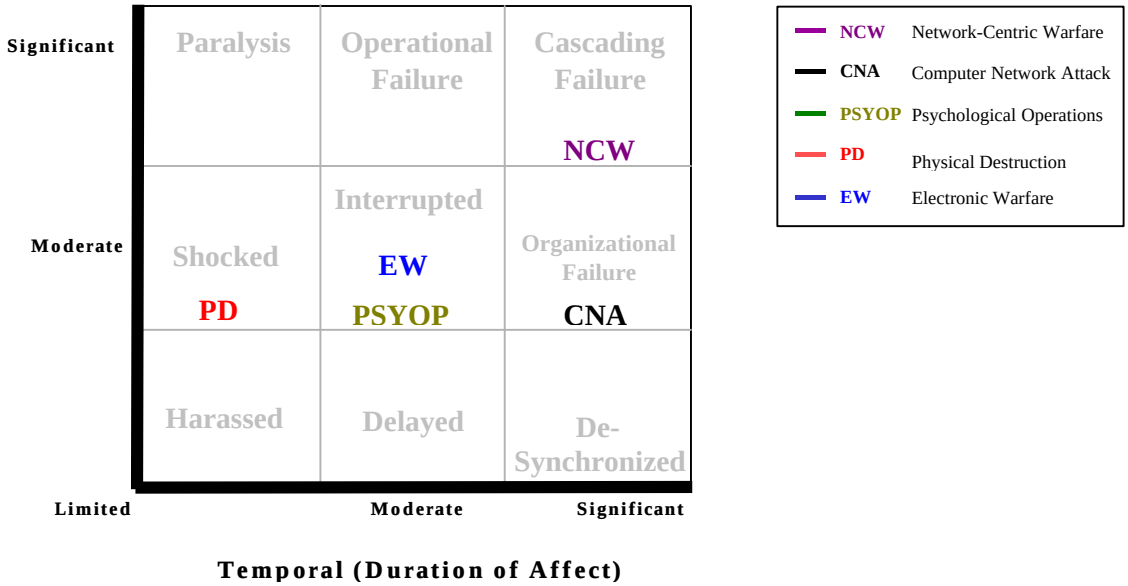
Function	PD	EW	PSYOP	CNA	NCW
Intelligence	●	△	●	△	■
Sense	●	△	●	△	■
Command	■	△	■	■	■
Communicate	△	■	■	△	■
Move	■	△	●	■	■
Sustain	●	△	■	■	■
Strike	△	△	△	△	■
Protect	■	■	●	△	■
Recovery Reconstitution	●	△	■	■	■

■ **Significant effect**
△ **Moderate effect**
● **Minimal effect**

Note: The first 4 functions are temporal,the last 4 are physical functions, Move is both.

The chart above describes a notional operational effects of physical and IW attacks against enemy functional capabilities[24]. The first column outlines the effects of Physical Destruction (PD), with minimal, moderate and significant scores given to each adversary's functional areas. The middle columns outline the same effects for IW operations, including Electronic Warfare (EW), Psychological Operations (PSYOP), and Computer Network Attack (CNA). The last column demonstrates the potential effect of synchronizing PD and IW attacks through Network-Centric Warfare (NCW) concepts. In all cases of analysis, the impact increases to a significant operational impact level.

[24] This chart, as well as the other two in this section, were derived from a Booz•Allen study in support of OSD/Net Assessment's Information Warfare Net Assessment. A more detailed discussion and description can be found in a SECRET document entitled "The Impact of Information Warfare on a



Synchronization of Physical & Mental Effects

The Synchronization of Physical & Mental Effects metric from the previous page displays the data from the above chart in a matrix format. The x axis represents effect duration, from limited to significant. The y axis reflects the total percentage of an adversary's force affected, from limited to significant. The background boxes within the matrix represent the combined physical and temporal effects suffered by the enemy. For example, significant physical effects for a limited duration results in paralysis. Conversely, limited physical effects for a significant duration results in de-synchronization. The effects inflicted on an adversary in each matrix box are summarized in the box illustrated below.

The operational effects of Physical Destruction, EW, PSYOP, CNA, and their combination represented as Network-Centric Warfare (NCW), are overlaid on top of the effect matrix in the form of their placement in the appropriate box in the matrix. These placements are arrived at through assessing the combined impact of the rankings from the first chart across the force and temporal functions. The y axis indicates the total physical effect and the x axis indicates the total affect duration. Each of the four methods can only create a moderate effect on the y-axis, though the CNA can by itself have a moderate impact over significant duration (cascading failure). When Network-Centric Warfare (NCW) combines and integrates all these capabilities into a single campaign (PA, CNA, PSYOP, EW), it is capable of creating significant operational impacts to both the physical and temporal and physical functions of the enemy and cause a cascading failure to their OPLAN.

Harassed: Warplans and operational outcomes are subject to minimal risk beyond that associated with normal friction.

Delayed: Ability to coordinate available forces is significantly reduced for a brief period.

De-Synchronized: Ability to coordinate available forces is significantly reduced for an extended period.

Shocked: Portions of forces critical to warplans and operational outcomes are significantly reduced for a short period.

Interrupted: Warplans and operational outcomes require significant modification to mitigate risk of failure.

Organizational Failure: Failure to coordinate portions of available forces for extended period.

Paralysis: Forces critical to warplans and operational outcomes are significantly reduced for a short period.

Operational Failure: Forces critical to warplans and operational outcomes are significantly reduced for an extended period.

Cascading Failure: Warplans and operational outcomes are at significant risk of failure

ii. Conclusions

Though this chapter highlighted 13 possible metrics for measuring the reason aspects of Network-Centric Warfare, several of them appear to be more critical to the ongoing study of the concept. First, it is difficult to envision a successful application of NCW without the necessary quality of information. Specifically, NCW is not possible without assured information accessibility, commonality, and velocity. Many of the advantages hypothesized for a force operating in a net-centric environment require near-constant access to consistent and timely information. In addition, the information needs to be precise to enable the accurate application of force or maneuver necessary to gain the desired advantage and outcome with dispersed forces.

Given the critical reason metrics discussed above, the key vulnerabilities and, by extension, potential dangers for a net-centric force concern the availability and integrity of the information flowing through the system. There are two main options for an enemy seeking to disrupt the flow and content of information: denial of service and manipulation of data. Clearly, denying information to fielded forces currently offers the enemy the highest probability of success and widest range of options, from electronic warfare targeting either the sender or receiver to destruction (lethal or non-lethal) of the data or key links and nodes in the network. Data manipulation requires a greater knowledge of, and access to, the target networks. However, altering the data does offer the attacker a variety of options from stealthily changing only a few critical pieces of information to corrupting the majority of the data to degrade the trust of the commanders and/or force them to operate without the expected quantity and quality of information.

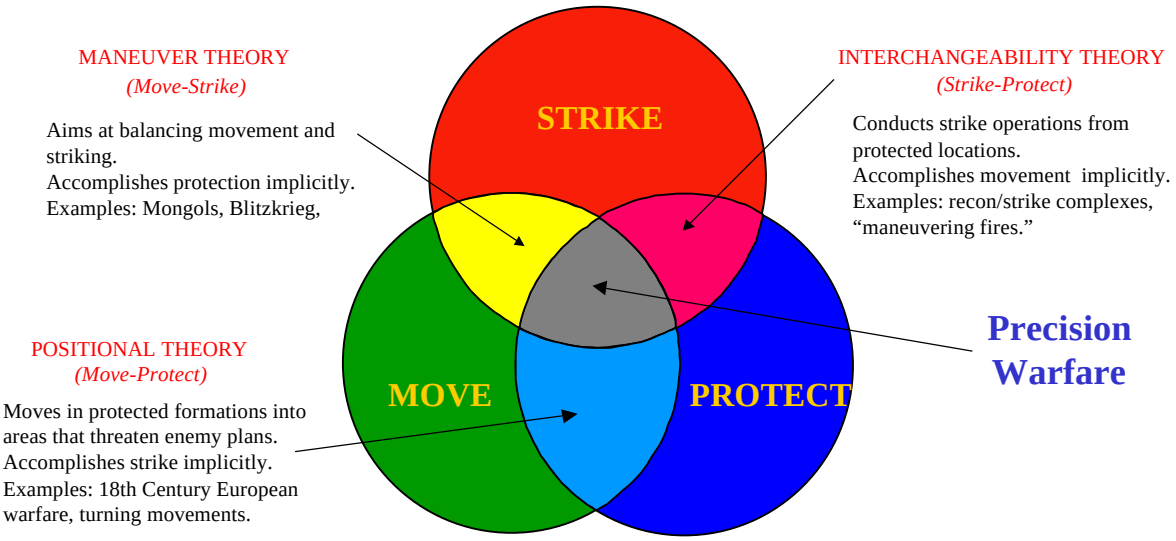
Finally, it should be noted that the highlighted reason metrics can be modeled/measured with several of today's analytic tools. The success or failure of these information attacks can be ascertained using the Entropy-Based Warfare Model™, as it has done for the Title X Wargames for the last several years. The EBW Model can determine when an attack is successful, the length of time the attack effected the system, and the negative effects they had on the network. In terms of network performance, there are an ever-growing number of analysis tools (including OPNET and ADVERSARY) which can monitor the efficiency and effectiveness of a variety of information systems as they operate under normal as well as degraded circumstances.

CHAPTER 7 PHYSICAL METRICS

> *"The military machine … is in fact simple, and appears on this account easy to manage. But let us reflect that no part of it is in one piece, that is composed entirely of individuals, each of which keeps up its own friction in all directions. The battalion always remains composed of a number of men, of whom, if chance so wills, the most insignificant is able to occasion delay and even irregularity."*
>
> Carl von Clausewitz, *On War*

ii. Introduction.

In warfare, the physical metrics are divided into three operational areas: move, strike, and protect. Movement involves the ability to transport units and platforms into the battlespace or around the battlespace in order to engage or avoid the enemy. Strike is the ability to use direct and indirect weapons against enemy targets. Protect is the ability to prevent, or mitigate the effects, of enemy movements or strikes against friendly forces.



In the physical sphere of warfare, these three operational areas occur within the dimensions of *force, space and time*. Force is normally defined as the tangible dimension of military power. It is comprised of the lethality or "combat punch" and the equipment associated with a particular unit or platform. Space is defined as the position, or distribution, of forces within the air, land, surface, and subsurface environment. The spatial dimension captures battlespace volume and relative positions of forces. The temporal dimension is reflected most notably in command and control but also permeates the time required strike or move as driven by the OODA loop. The time dimension captures the ability to rapidly execute movement and strikes against critical enemy nodes, thus creating the shock of closely coupled events and "locking out" enemy actions. Move, Strike and Protect are focused on the application of force within the battlespace, within the dimensions of force, space and time.

PHYSICAL METRICS

MOVE	*STRIKE*	*PROTECT*
• Effectiveness ❑ Asymmetric Force Advantage ❑ Local Force Advantage • Robustness ❑ Dispersion • Efficiency ❑ Speed of Command ❑ Convergence ❑ Self Synchronization	• Effectiveness ❑ Concentration ❑ Impedance • Robustness ❑ Variegation ❑ Spatial Propagation • Efficiency ❑ Massed Effects ❑ Weapons Responsiveness	• Effectiveness ❑ Preemption • Robustness ❑ Force Protection ❑ Dispersed Operations ❑ Security • Efficiency ❑ Effect Mitigation

ii. Move.

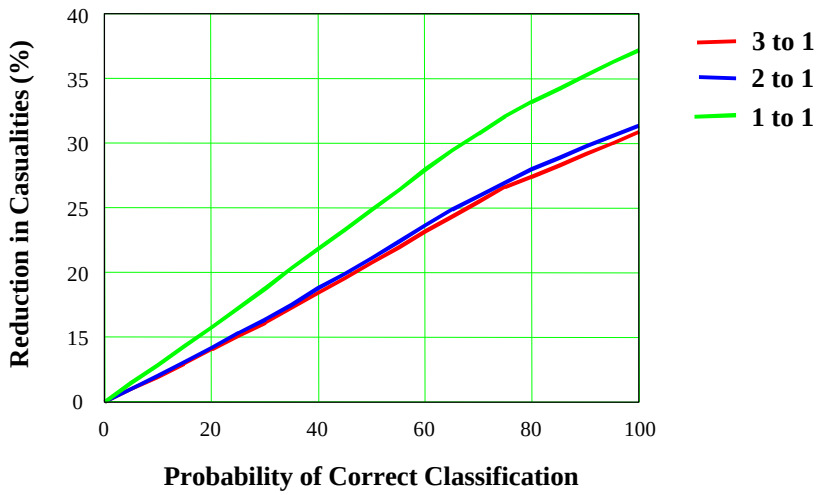
7..1 Effectiveness.

Effectiveness quantitatively captures the intended or expected results of systems or operational improvements. Specifically, move effectiveness quantifies improvements in force positioning within three dimensional space. An effective force moves, or positions, weapons systems to exploit enemy weaknesses (asymmetry) and to gain a favorable numerical force advantage (local force advantage).

Asymmetric Force Advantage.

An Asymmetric Advantage is represented by a lack of proportion between opposing forces. An Asymmetric Force Advantage is the capability to bring an asymmetric weapon system to bear upon an intended target. If a force can increase information accuracy through networking sensors and data, then it can precisely identify and classify enemy weapon systems, resulting in effective pairing of operational strengths against enemy weaknesses. By correctly classifying enemy forces, the most effective weapon can be brought to bear. For example, if a tank company is known to possess T-80 tanks, then an asymmetric force advantage would be helicopters or anti-tank weaponry, as opposed to a proportional tank-on-tank engagement. The metric is friendly casualties as a function of information accuracy (probability of correct classification).

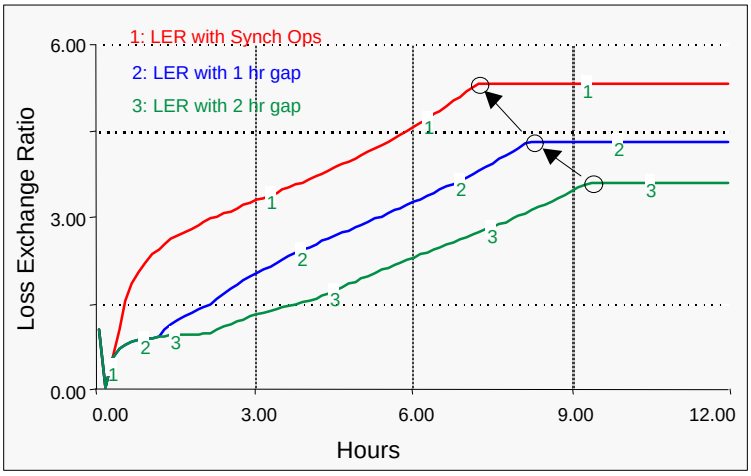
Planning for the Assault stages within the operational example illustrates the need for asymmetric force advantage. A higher awareness of the enemy force disposition allows the ATF commander to better coordinate strike assets. The x-axis measures the US sensor grid ability to classify North Korean ground units (i.e. distinguish between Soviet style T-55 tanks and DPRK indigenously produced T-62 tanks). Thus the amphibious assault and ground commanders could better choose which strike assets to engage the DPRK forces. The commander with a greater ability to distinguish North Korean tanks might choose to maneuver the far superior M-1A tanks against tanks known to be T-55 tanks. However, a commander not knowing which tanks he would be engaging, might maneuver attack helicopters against tanks that could be T-55 or T-62s to ensure victory with minimum casualties. The greater ability of a commander to match asymmetrically stronger US forces against the DPRK forces will experience greater reductions in US casualties.



Asymmetric Force Advantage

<u>Local Force Advantage</u>. Local Force Advantage is gained by positioning sufficient strength in a concise area in order to gain a numerical or capability advantage. If a unit can increase its knowledge of enemy locations and intentions through its sensor grid and network, then it can maneuver forces to a decisive point of its choosing, resulting in an effective force advantage. A Local Force Advantage insures sufficient strength will be applied to a key defensive position or critical objective in order to achieve operational objectives. The <u>metric</u> is the ratio of friendly losses to the enemy over time as a function of enemy capabilities to reinforce and counter friendly execution.

For example, Phase IV of the operational example illustrates the impact of local force advantage. During the Ship-to-Shore and Air Assault Landings, landing crafts, V-22s and CH-46Ds rapidly maneuvered assault troops to various positions on the landing site. A significant local force advantage was created when the amphibious assault forces synchronized maneuver and firepower to create the largest possible force ratio at a specific point in time (illustrating the concept of dominant maneuver). The US troops were able to obtain a local force advantage over the DPRK infantry and armored forces under the protection of US off-shore and airborne offensive and defensive shooters. Using notional data the attached graph illustrates the impact of time latencies on the ability of US forces to achieve a local force advantage and the resulting loss-exchange-ratios. During the course of the assault, the blue losses relative to red losses were dramatically improved with fully synchronized operations. A time delay or location



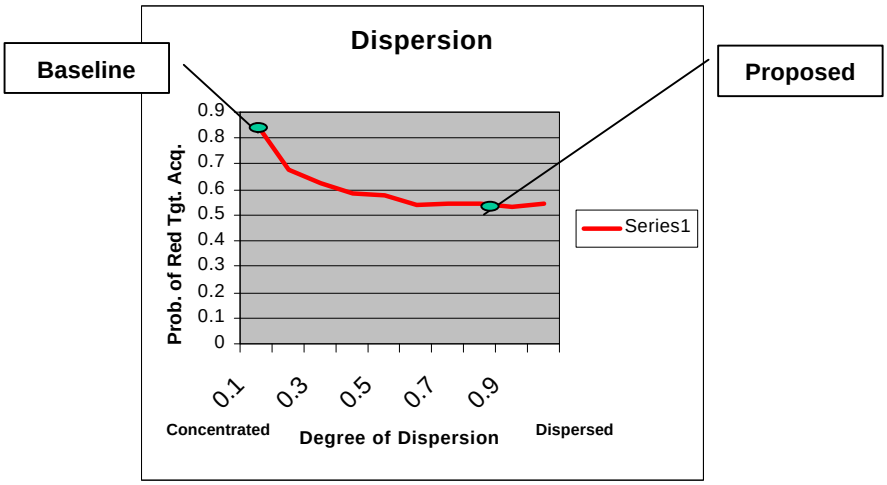
Local Force Advantage

error in arrival within the operational example would have prevented sufficient effective blue superiority over the DPRK forces in place.

7..2 Robustness.

Robustness is a measure of the overall health of a system. It implies the ability to avoid or absorb damage with minimum operational impact. Robustness is associated with depth, strength, and redundancy. Specifically, move robustness quantifies the ability of a force to absorb damage and continue towards its objective. NCW further allows a robust force to move with a high level of dispersion, limiting the effects of enemy precision engagements.

Dispersion. Dispersion is characterized by the capability to distribute forces across a geographical area while maintaining cohesion and effectiveness through NCW. If a force can increase its knowledge of enemy locations and intentions through its networks, then they can reduce the need for operational security and force concentration, resulting in lower probabilities of enemy target acquisition. Dispersed forces are harder to locate, identify, and classify, reducing the probability of enemy engagements against friendly centers of gravity. The metric is the probability of enemy target acquisition as a function of friendly force concentration.



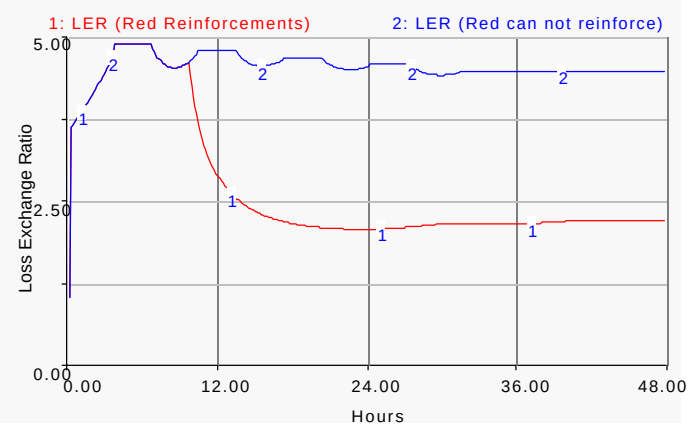
Dispersion

Dispersion is a common trait throughout the operational example. This metric is especially prevalent during the Pre-Assault stages of the operation. The blue amphibious task force approached the landing zone in a non-traditional dispersed formation. This degraded the DPRK's ability to detect and classify the blue naval vessels until the assault was imminent. The graphic on the previous page represents the Amphibious Task Force (ATF) adherence to a concentrated formation during the Pre-Assault stage in which the x-axis represents the relative dispersion (from traditional carrier battle group formation to non-overlapping sensors formation). Because the ATF was more dispersed, the probability of each vessel remaining undetected and unclassified by DPRK forces decreased until blue vessels began to engage surface targets.

7..3 Efficiency.

Efficiency is the ratio of work accomplished or energy expended relative to material inputs or time. In short, it is the accomplishment of a task with minimum expenditure of time and effort. Specifically, move efficiency quantifies the ability of a force to execute position changes rapidly in time. An efficient force executes commands swiftly (speed of command) in a coordinated manner (self-synchronization), enabling simultaneous movement toward a specific point in space (convergence).

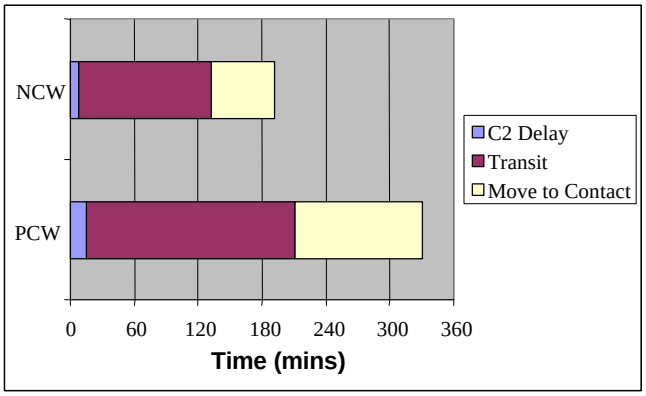
Speed of Command. Speed of Command measures the ability to issue and execute commands swiftly. If a commander can increase the velocity of information through its networks, then he can execute commands more efficiently in time, resulting in increased operations tempo. Speed of command allows a commander to act within an enemy's decision cycle. This enables proactive execution, limiting the opportunity cost spent reacting to enemy operations. The metric is friendly losses over time as a function of enemy capabilities to reinforce and counter friendly execution.



Speed of Command

For example, the Preparation of Sea and Beach Area Phase of the example scenario illustrates the principles of the Speed of Command metric. The ability of US ground and naval commanders to plan and coordinate their attack of DPRK ground units in near real-time (8sec-20min) decreased the ability of the red forces to coordinate a significant resistance to the blue assault. Using notional data, the relationship of Speed of Command and blue vs. red loss exchange ratios (LER) is illustrated in the above metric. While the Allied commanders were able to operate within the red decision loop, the DPRK artillery was only able to inflict minor damage; however, the synchronized blue forces were able to establish an approximate 4.75:1 LER advantage over the course of the operation. Had the blue ground and naval forces not been able to capitalize upon its faster command cycle, the LER over the course of the operation would have fallen to approximately 2.25:1 because the DPRK was able to reinforce its artillery forces.

Convergence. Convergence is marked by a coordinated movement toward a point, or objective. If network-centric warfare can provide a force with a common operational picture to maneuvering units, then that force can efficiently coordinate and de-conflict movement, resulting in movement toward an objective more rapidly in time. Convergence enables widely dispersed maneuvering force elements to swiftly coordinate movement toward a desired point. The metric is the distance moved toward a coordinated point as a function of time.



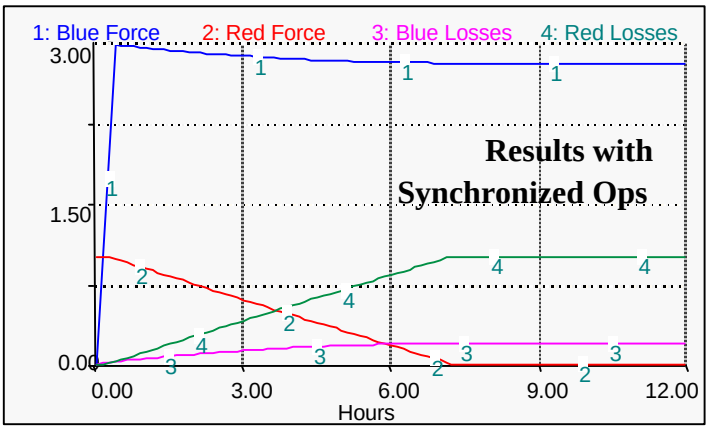
Convergence

Convergence is evident throughout the operational example. Using notional latency data, the attached metric illustrates the impact of a network-centric system in rapidly coordinating maneuver of US amphibious assault forces and US Army forces. During the Ship to Shore and Air Assault Phase of the example, command and control latencies associated with preparing and coordinating the ship-to-shore movement with the necessary supporting artillery fire from the US Army units was minimized. A minimal "build-up" period allowed a rapid transition from transporting US forces ashore to engaging the DPRK forces. The rapid assault of air transported forces aboard the V-22s and CH-46Ds, and the coinciding support from US ground artillery units, complemented the fluid

ship-to-engagement process for the amphibious forces. The minimal C2, transit, and move-to-contact times allowed the coordinated attack to engage the DPRK forces while they were still within transportation corridors restricted by damaged and destroyed LOCs and bridges.

Self Synchronization. Self Synchronization is highlighted by the ability of individual entities to coordinate actions horizontally at the same time, without top-down command. It is the ability to execute a commander's intent with unity of action across units and platforms. If NCW can provide common situation awareness to maneuvering units through its network architecture, then those units can self-organize their activities through lateral coordination between moving elements, resulting in simultaneous actions. Self-Synchronization creates unity of action through information commonality. The metric is the ratio of friendly losses to enemy over time as a function of simultaneous US actions over time.

The synchronization metric reflects the impact of self-coordination amongst the US ATF and Army forces. The attached chart reflects the attrition of DPRK forces within Phase IV of the operational example due to the self-synchronization of US forces. The x-axis is the timeline of the assault; the y-axis measures the force strength of US and DPRK forces. As the fighting progressed, the DPRK forces suffered increasing losses as US Army maneuver brigades and US amphibious units independently coordinated the focus of their attack on the North Korean infantry.



Self Synchronization

ii. Strike.

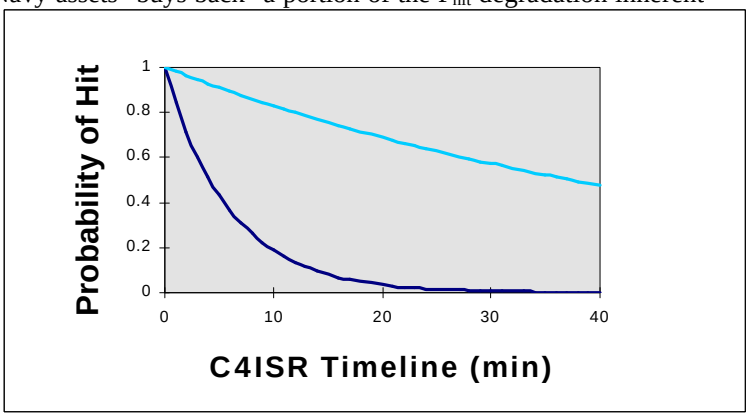
7..1 Effectiveness.

Effectiveness quantitatively captures the intended or expected results of systems or operational improvements. Specifically, strike effectiveness quantifies improvements in precision engagements. Precision engagement focuses on delivering the desired effect through the use of precision weaponry and stealth technologies, while minimizing collateral damage and the risk to friendly forces. The goal of precision engagement is to rapidly bring firepower to bear on a desired target, or targets, thereby shaping the battlespace. An effective force executes precision engagements through concentrating force on the desired target (concentration), while conversely impeding enemy precision engagement capabilities (impedance).

Concentration. Concentration is measured by the amount of energy concentrated in a given area or volume. If networked sensors increase target accuracy, it will increase the effectiveness of precision munitions through reduced target location errors, resulting in more effective engagements. A smaller force applied in a confined space is synonymous with a greater force applied to a larger area. Massing force (energy) in a small space maximizes effects (destruction). Concentration is maximizing energy while minimizing space. For example, World War II era bombing was very imprecise, dealing with huge target location errors. Therefore, enormous amounts of energy (carpet bombing) were required to effect a desired outcome (rendering a factory inoperable). Conversely, Desert Storm era bombing was more precise by several orders of magnitude, benefiting from much smaller target location errors and an input of precision information. The result was precision effects (precision guided munitions) delivered within a small volume

of space (a few meters). The metric is the amount of energy (megajoules) applied against a desired target as a function of a fixed volume of space (hectometers).

Phase III of the operational example (Isolation of landing area and local air superiority) illustrates the idea of concentration. The US Army AAA battery and USN destroyer both engaged the incoming North Korean helicopters with precise engagement munitions enabled by a common operational picture. This simultaneous employment of US firepower resources on a common objective increased the US probability of hitting the incoming DPRK helicopters. The attached metric illustrates the P_{hit} against North Korean helicopters with respect to the US C^4ISR sensor-to-shooter timeline. Within the network-centric system, the simultaneous response of US Army and Navy assets "buys back" a portion of the P_{hit} degradation inherent to traditionally increased latencies of targeting information. As the targeting latency increases, the ability to strike the incoming helicopters decreases; however, by concentrating attack, the degradation is minimized.

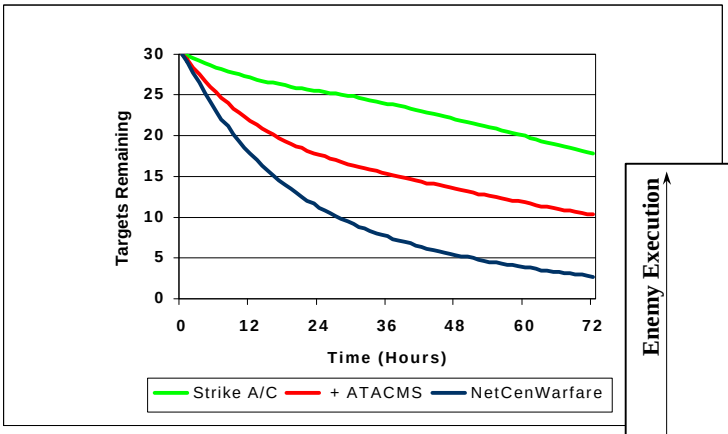


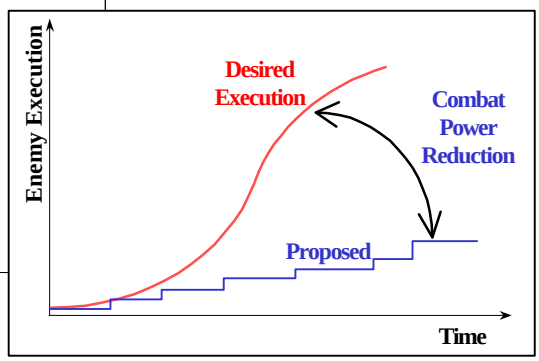
High level of concentration (NCW)

Low level of concentration Baseline (PCW)

Concentration

Impedance. Impedance interferes with and slows the progress of enemy execution by applying precision force to enemy centers of gravity at the key time and place. If a force can gain knowledge of enemy intentions through its networked sensor grid, then they can target enemy functional centers of gravity, resulting in effective impedance of enemy engagements. Impedance creates disruption within the enemy's decision cycle by destroying critical nodes at a key point in time. Impedance uses the network to coordinate execution across service and platform boundaries in order to strike the right targets at the right time. Precision engagements are used against key enemy nodes, forcing increased enemy planning, coordination, de-confliction and synchronization over time. As a result, enemy execution is repeatedly delayed over time. The metric is combat power reduction as a function of enemy execution over time.





Impedance

Within the initial phase of the operational example (Destruction of enemy forces ashore), the US concentrated on DPRK search radars, fire control radars, C2 nodes and other targeting assets. This coordinated assault exemplifies the metric of impedance. The above plots trace the impact of attacking key

North Korean targeting nodes on the DPRK's ability to detect and destroy the US naval and ground forces. The first chart depicts the time within the first phase during which the key targets were attacked. The second chart measures the resulting ability of DPRK forces to engage US forces as their targeting assets are attacked. Integrating the plots illustrates the degraded ability of the North Korean forces to engage US forces as the US destroys key nodes as a result of the Allies' successful impedance.

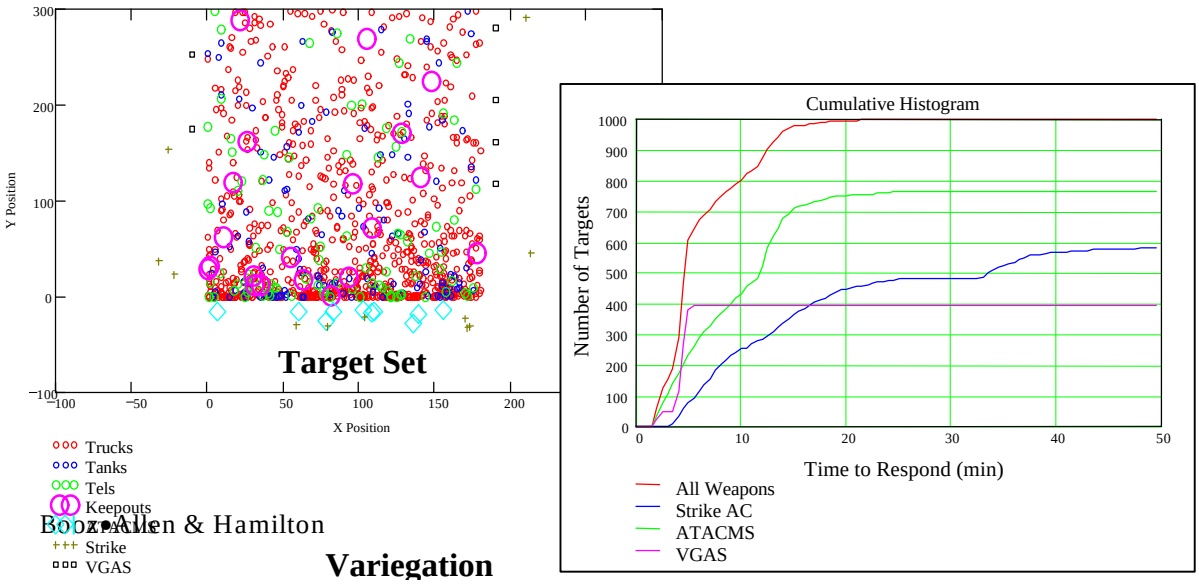
7..2 Robustness.

Robustness is a measure of the overall health of a system. It implies the ability to avoid or absorb damage with minimum operational impact. Robustness is associated with depth, strength, and redundancy. Specifically, strike robustness quantifies the ability to successfully strike the enemy after absorbing damage through maintaining a wide variety of strike capabilities and through holding enemy territory at risk. A robust force mitigates enemy engagements through distributing strike capabilities amongst a variety of platforms (variegation) and by holding enemy territory at risk through dispersion of strike assets (spatial propagation).

Variegation. Variegation measures the variety of weapons systems capable of applying force to a desired target to cause physical destruction. If a force can maintain all its precision weapons as nodes connected to a network, then it can efficiently pair weapons with targets, resulting in effective force variegation. A highly variegated force has strike capabilities distributed amongst a variety of platforms. A force with low variegation levels maintains strike capabilities in only a few platform types. For example, a battle force composed of a single guided missile cruiser would have a great deal of strike capability (over 1,500 precision rounds). However, the variegation level would be low because the ship represents a single point of failure. Conversely, a battle force composed of ships, aircraft and surface-to-surface missiles would have a high level of variegation because strikes may continue to be executed even as the level of friendly attrition increases. The metric is the number of targets held at risk over time.

In the graphic below, the chart on the left illustrates the potential DPRK laydown and the positioning of US assets during the fight for the littoral regions within Phase V (Ship-to-shore and assault landings). By employing a combination of ATACMS, TLAMS, and VGAS the joint US forces were able to individually hold many of the North Korean forces at risk as evidenced by the y-axis of the chart on the right. By integrating the US assets under a common operational picture, the cumulative North Korean forces held at risk by multiple assets increased as evidenced by the "All Weapons" line of the right chart. At the same time, the US forces were able to absorb losses without a proportional loss in DPRK targets held at risk because of the integrated fire control and battle management.

Spatial Propagation. Spatial Propagation represents the capability to hold physical area at risk for strike

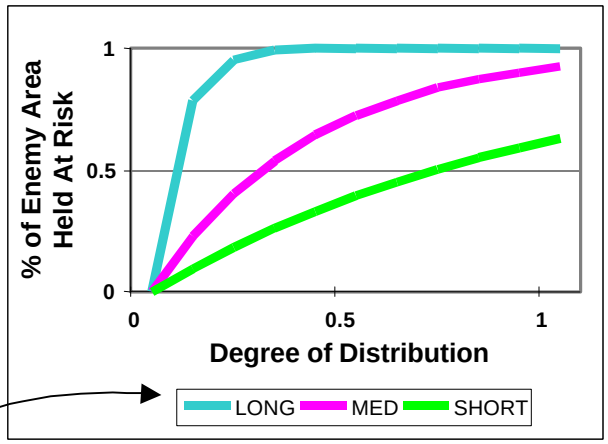


Booz Allen & Hamilton

Variegation

assets. If networked sensors can gain a high degree of situation awareness, then a commander can position strike assets to efficiently range enemy territory, resulting in effective weapons response. The placement and positioning of precision engagement assets determines the quantity of enemy territory covered. It is a function of weapon ranges and capabilities to hold key enemy nodes at risk to engagement. Spatial propagation enhances strike flexibility by providing opportunities to engage the widest possible target array, resulting in spatial dominance of the battlespace. The metric is the quantity of enemy area held at risk as a function of weapon distribution.

The operational example scenario illustrates spatial propagation as an inherent need of a variegated force structure. Long range weapons, such as the Tomahawk cruise missiles used in Phase I, consistently held high percentages of the DPRK defenses at risk. On the other hand, shorter-range weapons, such as ERGMs and 105/155mm artillery require a greater degree of dispersion to continuously hold a high percentage of North Korean targets at risk. The x-axis of the graph indicates the degree to which the US amphibious assault is dispersed. An example of a non-dispersed assault would be if the US destruction of DPRK defenses ashore were strictly performed by naval platforms in a traditional ATF or CVBG formation. The other end of the axis represents engaging the DPRK from dispersed Navy platforms from the sea as well as from US Army units along the FLOT. The result is that the more dispersed attack formation is able to engage a higher percentage of the DPRK units more rapidly.



(Relative Range Class of Weapons Available)

Spatial Propagation

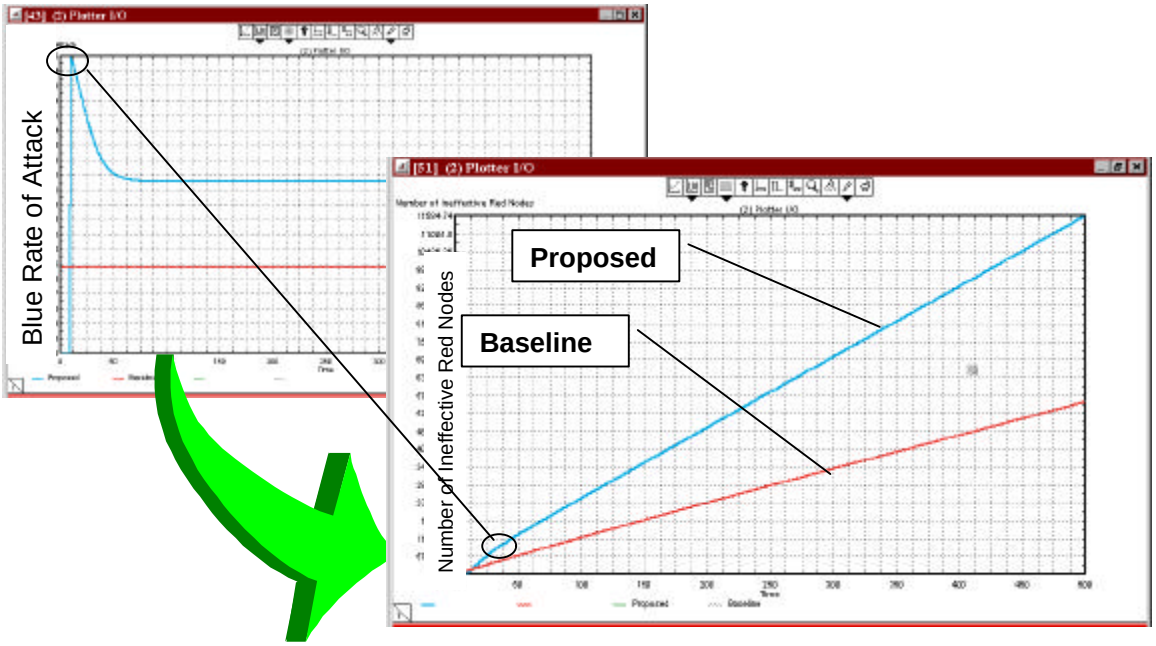
7..3 Efficiency.

Efficiency is the ratio of work accomplished or energy expended relative to material inputs or time. In short, it is the accomplishment of a task with minimum expenditure of time and effort. Specifically, strike efficiency quantifies the ability to rapidly execute precision engagements, while massing precision effects at the right time and place. An efficient force rapidly engages time critical targets (weapons responsiveness) while simultaneously massing precision effects on the desired target (massed effects).

Massed Effects. Massed Effects are characterized by the ability to mass fires, rather than massing forces. More precisely, it is the ability to mass precision effects in time (increased engagement tempo). If NCW allows the commander to rapidly plan, coordinate, and de-conflict strikes, then he can synchronize precision engagements in time, resulting in near simultaneous effects against the enemy. Precision effects (lethal and non-lethal) are delivered with simultaneity and are massed against the key enemy centers of gravity. Thus, Massed Effects are precision effects accurately delivered at the right time and place. Massed Effects will render a high number of key enemy centers of gravity ineffective in a compressed period of time – causing a disproportionate amount of disruption to the enemy. The metric is the number of enemy nodes rendered ineffective over time.

Within Phase II of the scenario, North Korean forces began to mobilize resistance to the quickly arriving US ATF. The heightened US awareness of North Korean maneuvering allowed US Army and Navy assets to simultaneously engage the DPRK ground units with rapid and intense fire. In the graphic below, the rate of firepower delivered on the North Koreans is indicated in the left plot. The dramatic number of DPRK forces hit within a small time window led to a disproportionately large number of DPRK units to be

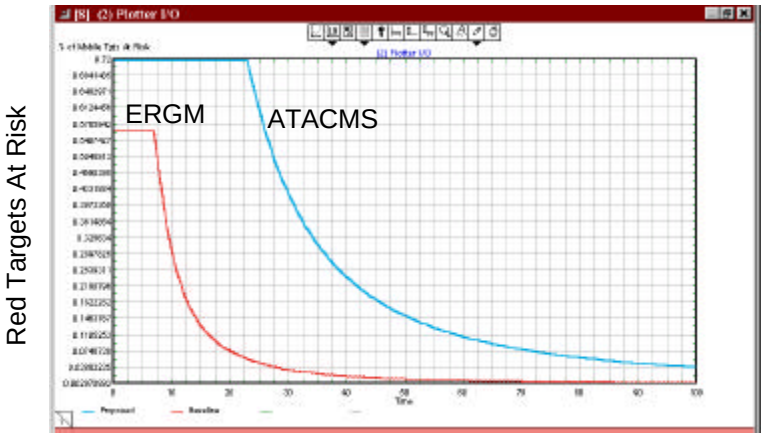
ineffective in their attempts to disrupt or degrade the avenues of approach of the US assault, as shown in the attached plot.



Massed Effects

<u>Weapons Responsiveness</u>. Weapons Responsiveness measures the ability of weapons to act quickly in order to engage time critical targets. If NCW allows a network to increase information velocity, it can provide near real-time (NRT) targeting information to the available shooters, resulting in effective engagements against time-critical targets. The ability to act rapidly is based upon information latency. The ability to engage is based upon kinematics and weapon position at a given point in time. For a weapon to be responsive, two criteria must be met. The first is position. The weapon system must be capable of engaging without sacrificing time to move into firing position. The second is latency. The command to fire and near real-time targeting information must be provided to the weapon system rapidly enough to engage the targets within the time window for that particular target (i.e., a Scud TEL). The <u>metric</u> is the number of enemy time critical targets held at risk as a function of information latency.

Facing several highly mobile Korean units, the operational tempo of the amphibious assault becomes largely a function of the rate at which information flows. The plot indicates the perishable effectiveness of weapons systems without NRT targeting information. The rapid timelines in which the US Army Patriot battery and US Navy AEGIS cruiser engaged the incoming TBMs in Phase IV of the scenario illustrate the benefit of a common relevant operational picture. The COP allowed US forces to operate within the munitions' time



Weapons Responsiveness

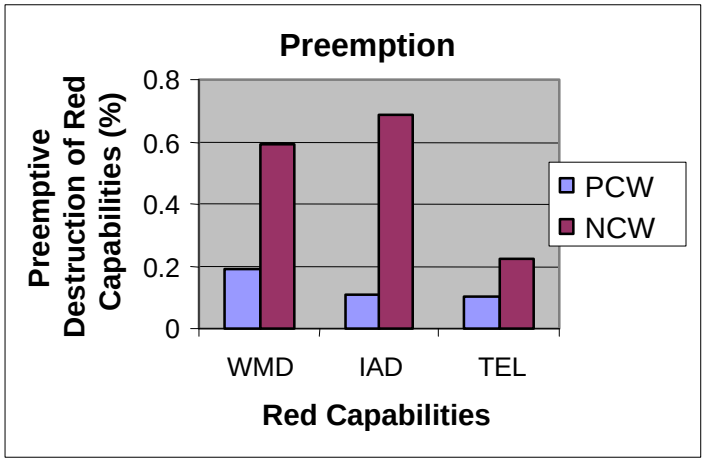
windows to defend against the incoming missiles, as illustrated by the attached plot.

ii. Protect.

7..1 Effectiveness.

Effectiveness quantitatively captures the intended or expected results of systems or operational improvements. Specifically, protection effectiveness quantifies the ability to deny the enemy engagement opportunities versus friendly forces or assets. It is characterized by preventing enemy action through the timely use of precision engagements against enemy capabilities. Effectiveness is also measured as a function of air, land, or sea control, limiting the offensive choices available to the enemy. An effective force protects itself through exercising direct influence over the battlespace (battlespace control) while proactively striking the enemy to prevent them from taking offensive action (preemption).

Preemption. Preemption measures the execution of precision engagements to prevent the enemy from taking offensive action. Preemption is the ability to proactively strike specific enemy capabilities which hold blue targets at risk. A network can identify high value targets through ubiquitous sensor access, then a commander can proactively target enemy precision engagement capabilities, resulting in effective denial of enemy asymmetric advantages. Specifically, preemption focuses on eliminating enemy asymmetric capabilities before they are employed against friendly forces. Preemption ensures enemy precision engagements will not occur, or will occur with reduced effectiveness. For example, the capability to accurately identify and classify chemical weapons at an enemy airfield in a timely manner provides the opportunity to preempt the airfield, thus denying the enemy a chance to employ an asymmetric capability. Effective preemption provides force protection through asymmetric denial. The metric is the percentage of enemy asymmetric capabilities preempted (before they have an opportunity to act) as a function of precision engagements.



Preemption

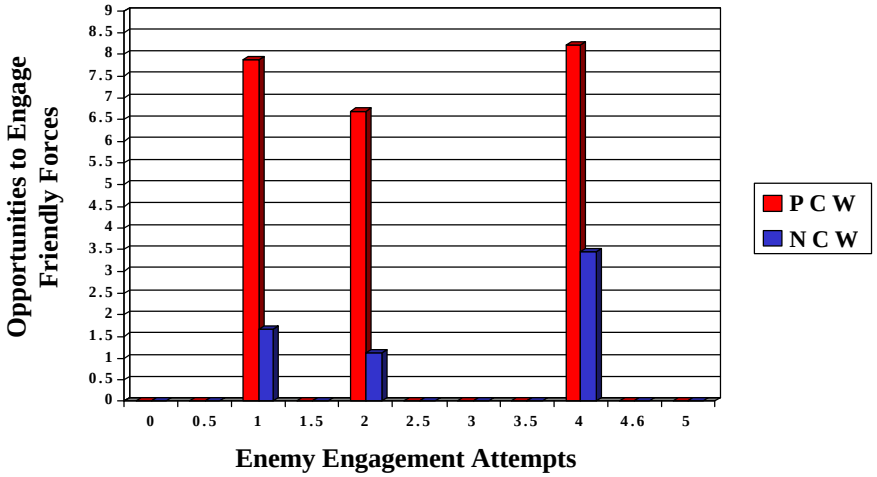
Various phases of the operational example illustrate the value of preempting North Korean asymmetric offensive actions. Within the context of the scenario, preemption is enabled by the sensor grid created by US ISR assets within the naval and ground forces, the information grid which connects these forces, and the engagement grid created by the naval and ground fire capabilities. The ability to engage DPRK TELs is handicapped by the rapid move cycle of the targets. However, the ability of the integrated US assets to target WMD storage and deployment facilities and to systematically attack North Korean anti-ship missiles, air defense search and target radar, and the surface to air missile sites is significantly enhanced by the virtual sensor and shooter umbrella of networked US naval and ground forces.

7..2 Robustness.

Robustness is a measure of the overall health of a system. It implies the ability to avoid or absorb damage with minimum operational impact. Robustness is associated with depth, strength, and redundancy. Specifically, "protect" robustness quantifies the capability to protect friendly forces from enemy weapon systems and to absorb damage as a function of dispersion. A robust force protects itself by destroying penetrating weapon systems or WMD and limits damage through distributed capabilities.

Force Protection. Force Protection is measured as the ability to protect air, land and sea forces from enemy weapons system using defensive means. Enemy engagement attempts have the potential to penetrate these defenses, resulting in "leakers". A leaker is defined as any direct or indirect fire weapon system which has successfully penetrated defensive measures and has an opportunity to engage friendly forces. If NCW can connect sensors, radar, and weapons systems into a cooperative defensive network, then a force can successfully engage a greater number of enemy weapons systems at ever increasing ranges, resulting in fewer leakers. The metric is the number of leakers over time as a function of enemy engagement attempts.

The leaker metric ties directly to the Scud attack within Phase IV of the operational example. The ability of the AEGIS and Patriot battery systems to simultaneously detect, acquire and engage the TBMs illustrates the reduction in targeting and decision latencies created by a common operational picture. This accounts for the decreased ability of the North Koreans to engage US forces as indicated by the y-axis of the attached plot.

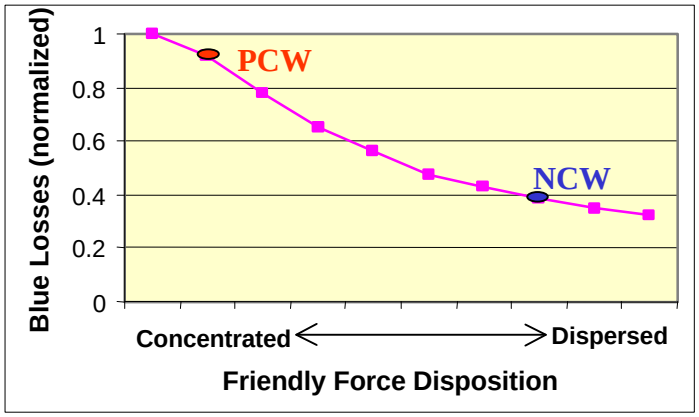


Leakers

Dispersed Operations. Dispersed Operations are characterized by spreading or distributing units away from a fixed or constrained area. Dispersed forces are not aggregated or clustered into a dense mass or formation. If a commander can gain knowledge of enemy positions and operational concepts through networking sensors, then we can conduct operations using dispersed forces, resulting in lower friendly losses to enemy engagement attempts. High levels of knowledge decrease the need for security and enable high levels of dispersion. Dispersed forces are harder to detect, minimize

mass for enemy targeting, degrade the effects of enemy fire, and deny capabilities to isolate centers of gravity. The metric is friendly losses as a function of the distance between targeted friendly force elements.

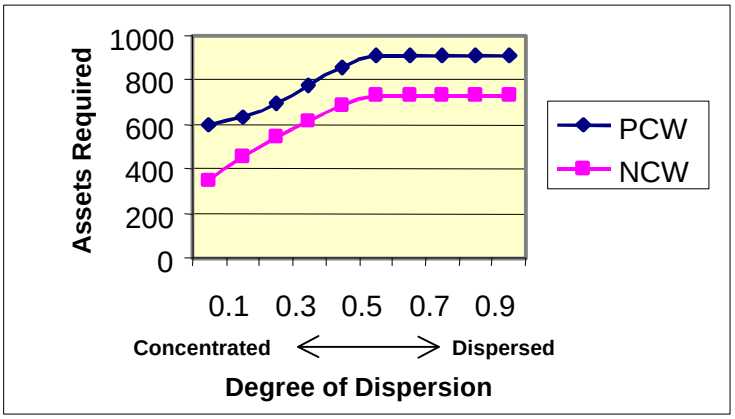
The formation of US forces impacts the ability of the North Koreans to engage the ATF and Army units. The assault began in Phase I while naval forces were still 100 nautical miles from the North Korean coast. In addition, the preparation of the sea and beach areas is accomplished by US naval and ground forces. The assault does not present a single "point of failure" to the North Korean forces. To impede the assault, the DPRK forces must engage discreet points of attack on land and at sea. The disaggregated units engaged in a common mission creates US lower casualties, as indicated by the y-axis of the attached graph.



Dispersed Operations

Security. Security measures the assurance against the threat of attack through force protection within an established area. Secure forces are protected by the threat of force. That is, they are defended by an offensive capability. Dispersed forces require more security due to their smaller numbers. Conversely, concentrated forces minimize the amount of force protection assets required. If NCW can gain knowledge of enemy positions and operational intent through networking sensors, then a commander can provide security with fewer forces, resulting in fewer friendly force protection assets required. The metric is the amount of force protection assets required to defend a fixed area as a function of dispersion.

Increasing the dispersion of the amphibious assault forces increases the potential risk to each individual ground unit and naval asset. A traditional close unit formation provides "safety in numbers." Within the amphibious assault scenario, a Perry class frigate is potentially endangered when it strikes a free floating mine because it is geographically dispersed from the other elements of the ATF. As the attached graph indicates, within a dispersed, platform centric ATF, the security of the frigate would depend on its organic assets; thus to ensure its security, it would require the



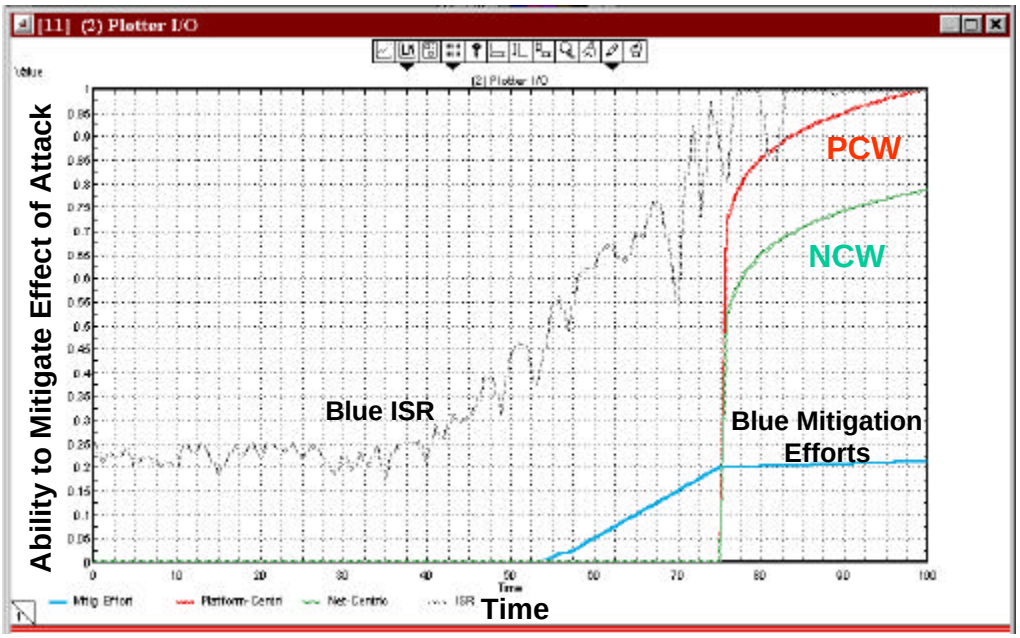
Security

assistance of increased force protection assets. However, with a network centric system, the Perry frigate's security is ensured by the collective targeting, C2, and firepower assets of the elements of the task force within effective range to cover the damaged frigate. The common sensor-information-shooter grids allows a dispersed force structure to maintain security under the protective umbrella of the collective system.

7..3 Efficiency.

Efficiency is the ratio of work accomplished or energy expended relative to material inputs or time. In short, it is the accomplishment of a task with minimum expenditure of time and effort. Specifically, "protect" efficiency quantifies the ability to delay or prevent the enemy from acting, and to limit the effects once the enemy decides to act. An efficient force increases the cost to the enemy every time he/she acts, thus increasing blue survivability.

Effect Mitigation. Effect Mitigation measures the ability to reduce the effects caused by enemy offensive actions. Effect Mitigation limits damage that will inevitably occur by increasing the response time of friendly forces. Increased warning time enables efficient response to impending attack. If NCW can provide timely indications and warning of impending enemy attack through an intelligence, surveillance and reconnaissance network, then a force can mitigate the damage inflicted, resulting in reduced effects. For example, providing timely indication of an impending enemy chemical weapons attack increases the response time for employing protective measures and postures, thus mitigating the overall effect of the attack. The metric is the ability of friendly forces to degrade the effectiveness of enemy attacks over time.



Effect Mitigation

Phase IV of the operational example provides the context for US forces mitigating the impact of DPRK aggressive actions. The TBM launch against US forces occurs within the extended coverage of the sensor grid. Thus while the ballistic missiles were on their boost phase, US ground and naval targeting and C2 systems began responding. Well before the expected impact would have occurred, the US amphibious forces on the ground are warned so that active and passive defensive measures can be employed. Using a notional TBM timecycle, the missiles are launched at t=45s. The increased warning which the Allied sensor grid provided is indicated on the attached chart at approximately t=50s. The information grid of the network centric system allows the US forces to quickly begin defensive measures at t=55s. The heightened awareness of the overall networked system allows the US to minimize damage of the Scud attack; whereas a less responsive system would potentially suffer greater losses.

ii. Conclusions

Though this chapter highlighted 17 possible metrics for measuring the physical aspects of Network-Centric Warfare, several of them appear to be more critical to the ongoing study of the concept: dispersed operations and asymmetric force advantages. The ability to operate forces in a more dispersed manner offers several unique benefits. First, it improves force protection by complicating the enemy's target acquisition capabilities by offering a smaller signature, spread out over a greater distance, while providing integrated protection covering all platforms. Second, it forces the enemy to divide its forces in an attempt to attack the dispersed force, reducing their firepower. Finally, it allows the dispersed force to attack the defender from a variety of angles complicating their defensive task. This asymmetry at the critical point allows for the generation of a local force advantage, which will allow smaller and more mobile forces to achieve their desired results against the critical components of large enemy.

The chief vulnerability to operating in such a manner is that the dispersed force could find itself at a local force disadvantage if the enemy is able to locate it and overcome or subvert the forces' integrated defenses. The notion that dispersed forces may evolve into "thin shooters" which may be less individually capable than today's ships, means that they will be less capable of defending themselves if they are forced to engage an enemy head-to-head. The same degradation in effectiveness can be ascribed to a thin shooter's non-synchronized attack, which would not be as powerful as today's heavier and more robust platforms.

There are a number of campaign and ISR models that assess the ability of a dispersed force to avoid detection and conduct synchronized attacks. However, new modeling approaches are required to accurately capture the impact of a generating a local force advantage that are not currently reflected in attrition-based models. The Entropy-Based Warfare Model™, which uses unit cohesion and effectiveness as its primary metrics, does offer hope that we can begin to simulate these effects.

CHAPTER 8 CONCLUSION

ii. NCW – Key Attributes.

Throughout the paper, a number of different attributes of NCW repeatedly surfaced during the analysis. The first key attribute of NCW is its ability to allow friendly forces to operate in a dispersed manner without sacrificing operational capability. A dispersed force complicates the enemy's targeting problems, which will only become more critical in the future as enemies continue to advance their sensor-to-shooter systems hence making it more robust. The second key attribute is the responsiveness offered by improved C4 and connectivity. Gaining the temporal advantage (turning information into effects faster) provides a commander with a much wider range of options than a commander forced to react. When the timeliness is combined with a networked force, the commander is then capable of orchestrating truly simultaneous operations. Finally, a Common Operating Picture will allow each unit on the network to respond to each of the threats reducing the overall potential risk, provided it depicts the information relevant to that particular threat. The response could come in the form of a self-synchronized force responding to each threat based on the commander's intent or reduce the incidences of friendly fire.

On the other hand, there was one particular vulnerability of NCW that also cuts across all facets of military operations. The vulnerability concerns the requirement to maintain the timely flow of information and communications through the networks. If the information is not available to the key commanders or units at critical time, then the lighter, dispersed forces will be in danger of being overpowered by traditionally deployed heavier forces.

ii. NCW – Key Metrics.

Though this paper highlighted over 30 possible metrics for measuring Network-Centric Warfare, several of them appear to be more critical to a useful study of the concept. These three sets of metrics are tied to the critical insights listed above:

- Information Accessibility, Commonality, and Velocity
- Information Integrity and Precision
- Dispersed Operations and Asymmetric Force Advantages

ii. NCW – Navy Integration of NCW

The Navy's integration of Network-Centric Warfare will take place in two stages. The first stage will see the new integrated architectures optimize the current Navy force structure. The improvements will likely be evolutionary vice revolutionary because the

force structure was not designed to specifically operate with these advanced network capabilities. The second stage will see a new force structure optimize the capabilities of the network. This second phase will feature a Network-Centric construct, integrated into a modernized force that will be optimized to take advantage of the improved capabilities.

ii. NCW – Next Steps.

5. All experiments should have an hypothesis. In the same vein an experiment should hypothesize metrics and the data required to calculate them. Notional data should then be used to generate the quantitative basis that supports the experiments hypothesis. This type of analysis should drive a Fleet Battle Experiment's data collection plan. Once the experiment is concluded, the data should be run back through the metric tools to generate the real results of the experiment and learn through comparison why the results differed. This approach will increase the value of the experiment.

6. Develop a more detailed understanding of the attributes and vulnerabilities of the systems that comprise a network-centric force. This needed detail should apply not only to the information and network systems, but also the capabilities of the forces to make maximum use of the potential of NCW. One way of generating experimental data for use with these metrics is through the conduct of Fleet Battle Experiments. Only by gaining a firmer grasp of the real capabilities can we begin to more accurately measure its effectiveness.

7. Explore the Belief aspects of warfare. Again, there is a consensus concerning the critical variables of morale, training, experience, leadership, etc. The problem is that analysts and modelers have not yet developed a method for quantifying these predominantly qualitative factors. This has historically been true warfare aspects such as command and control and the value of information, let alone assessing a soldier or unit's will to fight. There are some promising measures (training hours, man-hours, etc.) and models (Entropy-Based Warfare, Swarm, etc.) but a great deal more work is required before the analytic community will able to accurately represent these factors.

8. Assess an alternate force structure, based on NCW concepts, which features a move toward increased platform nodes based on smaller ship classes whose network creates a virtual capital ship. In the past this concept would have failed because an enemy capital ship would have dominated the smaller non-capital ships. However, with the benefit of the network, the combined capabilities of the ships using the COP would offer alternate force structure options which may optimize the benefits of NCW.

ANNEX A BIBLIOGRAPHY

Boslego, David V., *The Relationship of Information to the Relative Combat Power Model in Force XXI Engagements*. School of Advanced Military Studies, United States Army Command and General Staff College, Fort Leavenworth, Kansas, 1996.

Buck, B. and Macauley, V. eds. (1994). *Maximum Entropy in Action*. Oxford: Clarendon Press.

Cebrowski, Arthur and Gartska, John, *Network-Centric Warfare: Its Origin and Future*. Naval Institute Proceedings, 1997.

Çambel, A.B. (1993). *Applied Chaos Theory*, San Diego: Academic Press.

Cowan, G, Pines, D, and Meltzer, D. eds., (1994). Complexity: Metaphors, Models and Reality, Santa Fe: Addison-Wesley Publishing Company.

Czerwinski, Thomas J., *Coping with the Bounds: Speculations on Nonlinearity in Military Affairs*.

Einstein, Albert and Infled, Leopold, The Evolution of Physics: From Early Concepts to Relavitivity and Quanta, New York, Simon and Shuster. 1966

Fuller, J.F.C., *The Foundations of Science and War*. London; Hutchinson and Co., Ltd., 1926.

Herman, Mark, *Entropy Based Warfare: A Unified Theory for Modeling the Revolution in Military Affairs*. Booz-Allen & Hamilton, 1997.

Hill, T. (1986). *An Introduction to Statistical Thermodynamics*. New York: Dover Publications, Inc.

Ilachinski, Andrew, *Land Warfare and Complexity, Part I: Mathematical Background and Technical Sourcebook*. Center for Naval Analyses, July 1996.

Kibble, T.W.B. and Berkshire, F.H. (1996). *Classical Mechanics*. London: Longman.

Kuhn, T. (1962). *The Structure of Scientific Revolutions*. Chicago: University of Chicago Press.

Mainzer, K. (1996). *Thinking in Complexity: The Complex Dynamics of Mater, Mind and Mankind*, Berlin: Springer.

Prigogine, I and Stengers, I. (1984). *Order out of Chaos*, Toronto: Bantam Books.

Prigogine, I. and Kondepudi, D. (1998*) Modern Thermodynamics: From Heat engines to Dissipative Structures*, Chichester: John Wiley & Son