Information and Knowledge Centric Warfare: The Next Steps in the Evolution of Warfare

By Dr. Paul W. Phister, Jr. and Mr. Igor G. Plonisch

Point-of-Contact: Dr. Paul W. Phister, Jr.

Air Force Research Laboratory / Information Directorate

26 Electronic Parkway, Rome NY 13441-4514

VOICE (315)330-3315; FAX (315)330-7043

paul.phister@rl.af.mil; igor.plonisch@rl.af.mil

Information and Knowledge Centric Warfare: The Next Steps in the Evolution of Warfare

By Dr. Paul W. Phister, Jr. and Mr. Igor G. Plonisch
AFRL/IF, 26 Electronic Parkway, Rome NY 13441-4514

Abstract

Over the past 20-years, the military services have evolved from platform-centric to network-centric warfare. As they continue to progress in the Information Age, network-centric warfare is envisioned to evolve into information-centric warfare (some evidence suggests this evolution has already taken place.) This paper is meant to be thought provoking, in as much as it proposes the next step in warfare: transitioning from network-centric/information-centric to *knowledge-centric warfare*. Network-centric warfare is built around human and organizational behavior – a new way of thinking in terms of linkages. Its end result is combat power that can be generated from the effective linking or networking of the warfighting enterprise. Its premise is the ability to push "information to the edge." Once this premise becomes institutionalized, warfare will utilize the proven attributes of network-centric/information centric warfare to go to the next, logical, evolutionary step in the conduct of warfare -- namely pushing "knowledge to the edge". This next step is a transformation of network/information-centric-warfare's "Power **to** the Edge" to knowledge-centric warfare's "Power **of** the Edge". This paper discusses the basic tenants of network/information-centric warfare and how its' attributes form the basis for knowledge-centric warfare. Key technologies for the transition from network/information centric to knowledge-centric are discussed.

Introduction

Over the past 50+ years, there has been a major shift in the conduct of warfare. In WWII, the Allied Powers utilized large formations of B-17's. In Korea, this was reduced to formations of 4-6 aircraft. In Vietnam, F-4's flew in formations of 2-4. These formations were a result of established doctrine at the time, as well as tactics: they represented a platform-centric view of warfare.

As the military services entered the Information Age, doctrine and tactics changed to reflect rapid advancements in technology (especially in the area of information technology).

Network-Centric Warfare (NCW) is the current term used to describe the way the military services organize and fight in the Information Age. Network-Centric-Warfare is based on human and organizational behavior – a new way of thinking – a new mental model. Its premise is pushing "information to the edge" and its focus is on combat power that can be generated from the effective linking or networking of the warfighting enterprise[1].

[1] Alberts, David S, Garstka, John J., Stein, Frederick P., "Network Centric Warfare: Developing and Leveraging Information Superiority," CCRP, 2nd Edition, July 2002, page 2.

We posit that network-centric warfare will evolve into information-centric warfare. This, in turn, will evolve into knowledge-centric warfare as the military services move from the Information Age to the Knowledge Age sometime in the future.

Network Centric Warfare

NCW is a logical transition from platform-centric warfare. The focus of NCW is networking battlespace entities (e.g., platforms) so they can work in concert to achieve synergistic effects[2]. NCW is about human and organizational behavior. Alberts, etc. al., highlight the fact that NCW is based on adopting a new way of thinking-network centric thinking-and applying it to military operations. The structure of NCW (in 1999) as applied to military operations[3] is shown in Figure 1[4].

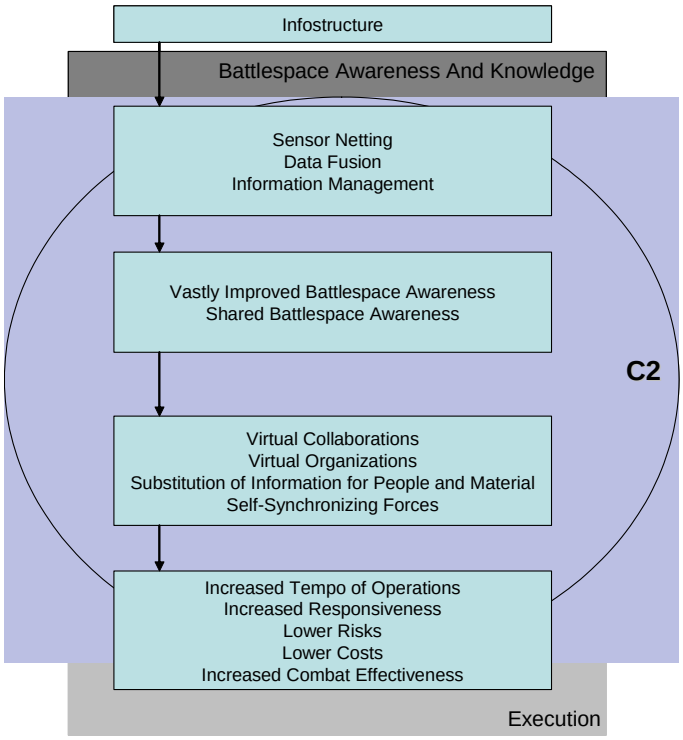

Figure 1: The Military as a Network-Centric Enterprise

This has evolved (2003) into the NCW/NCO Conceptual Framework as shown in Figure 2.

[2] Alberts, David S, Garstka, John J., Stein, Frederick P., "Network Centric Warfare: Developing and Leveraging Information Superiority," CCRP, 2nd Edition, July 2002, page 94.
[3] Alberts, David S, Garstka, John J., Stein, Frederick P., "Network Centric Warfare: Developing and Leveraging Information Superiority," CCRP, 2nd Edition, July 2002, page 88.
[4] Alberts, David S, Garstka, John J., Stein, Frederick P., "Network Centric Warfare: Developing and Leveraging Information Superiority," CCRP, 2nd Edition, July 2002, page 89.

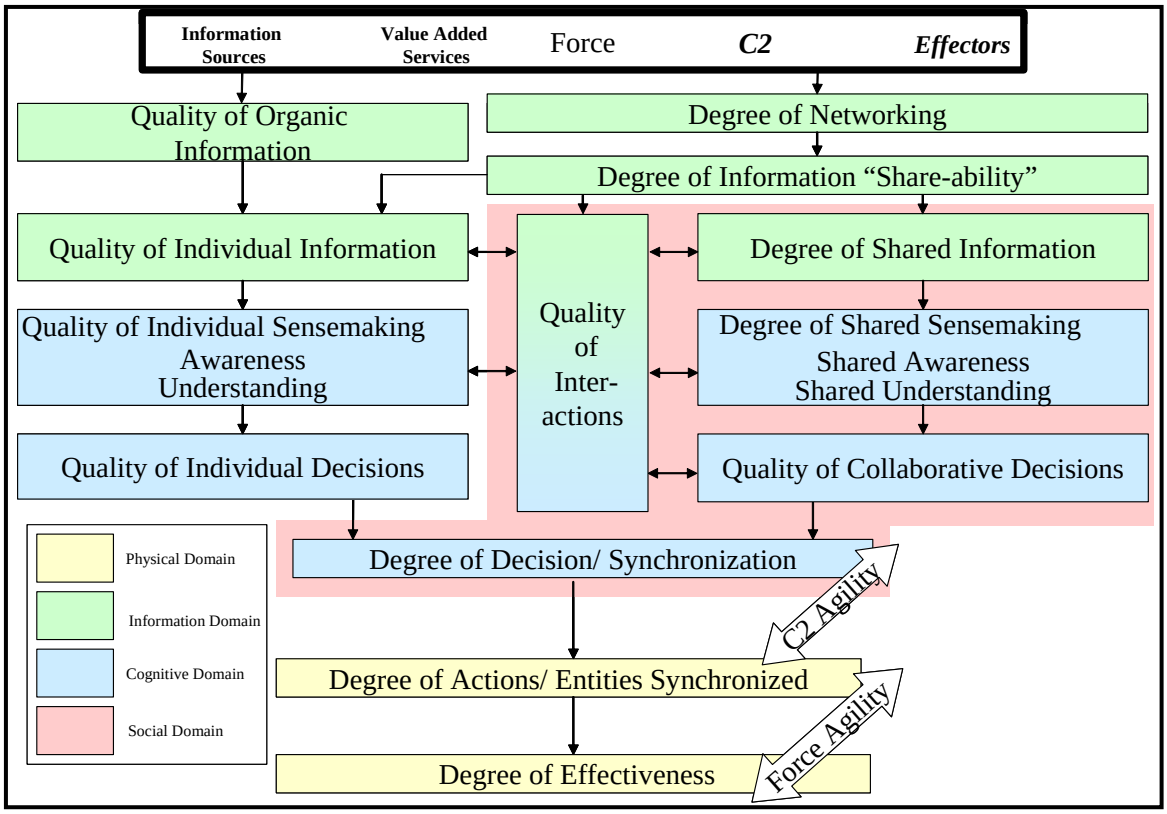

Figure 2: NCW/NCO Conceptual Framework

NCW has three attributes: "**Build** the net", "Protect the **net**", and "**Populate** the net" with the end goal of bringing "Power **to** the Edge". "Power to the Edge" is the ability of the total force to dynamically synchronize their actions in order to achieve Command and Control (C2) agility and increase the speed of command over a robust, networked grid that is not only well protected but allows any entity to join in order to achieve a strategic/operational/tactical mission objective. The goal is to shift the center of gravity out as far as possible in the network, in order to achieve effective military power.

Information Centric Warfare

Industrial Age C2 emphasized highly centralized planning and used linear and sequential processes in planning and executing military operations. Military organizations developed around that model featured numerous layers of command, and C2 technology tended to be "stovepiped," with the services fielding separate solutions to the problems encountered on the battlefield. "The principles underlying Industrial Age C2 remain important elements in today's U.S. military. . . The result is a joint C2 system that lacks agility and is largely inadequate to deal with the challenges of the future operating environment[5]," which will require enhanced information sharing and situational awareness. The 21st-century operational environment will place a heightened stress on joint C2, given uncertainties about where forces could be deployed

[5] **Joint Staff Officials Pushing Transition To Information Age C2 By 2015,** Inside the Pentagon magazine, November 14, 2003

next and increased demand for "high-quality information" from battlefield commanders and military officials who must work with their federal agencies and coalition partners. But today's joint C2 apparatus is not fully stuck in the Industrial Age. A wide range of information technology investments has resulted in a mixture of Industrial and Information Age approaches to C2 problems faced by warfighters. [6]

In Industrial Age C2, there was a limited variety of C2 systems available to the warfighter due to C2's unlinked and hierarchical nature. To meet the requirements of Ashby's Law[7], there must be low system variety. This is done by partitioning the battlespace into sectors, having specialised forces which focus only on particular optimized roles, and so on. This produces the balance shown on the left hand side of Figure 2, where Low C2 variety (or agility) matches low system variety.

In the Information Age, with networked capabilities (e.g., network-centric operations), there is a wider range of options available. This leads to better integrated and more precise actions and effects, and thus a better ability to deal with *asymmetric "niche" competitors.* Instead of probability of kill (the Industrial Age measure of attrition which enables the putting of strength against opposing strength) we have probability of options (the new Information Age measure which enables the maneuverist strategy of putting strength against opponent weakness). This is shown by the right hand side of Figure 3, where there is a high variety (agility) of the C2 system by design, matching the high variety of the complex and non-linear causal network of entities and their interactions.

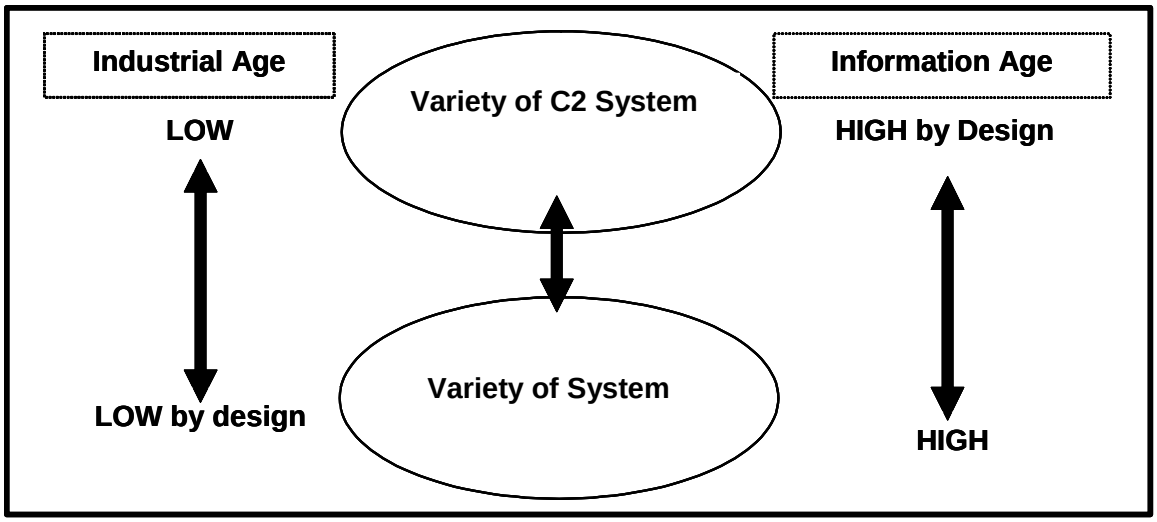

Figure 3: Ashby's Law of Requisite Variety and its Implications.

C2 elements span four dimensions of warfare (physical, information, cognitive, and social). C2 sensors, systems, platforms, and facilities exist in the physical domain. The information

[6] **Joint Staff Officials Pushing Transition To Information Age C2 By 2015,** Inside the Pentagon magazine, November 14, 2003

[7] *An Introduction to Cybernetics,* W.R. Ashby, 1957

collected, posted, pulled, displayed, processed, and stored exists in the information domain. The perceptions and understanding of what this information states and means exists in the cognitive domain, as well as the mental models, preconceptions, biases, and values that serve to influence how information is interpreted and understood, as well as the nature of the responses that may be considered. C2 processes and the interactions between and among individuals and entities that fundamentally define organization and doctrine exist in the social domain.[8]

Given the variety of elements involved in Information Age warfare and its effects-based orientation, command intent must be congruent across several elements (joint forces), coalition elements (combined), interagency partners, international organizations, and non-governmental organizations[9].

Using Figure 4, below, as a guide, one can see the migration, or transition, of warfare from platform-centric (predominately physical domain), to NCW (predominately physical and information domains) to ICW (predominately information domain) to KCW (predominately cognitive domain).

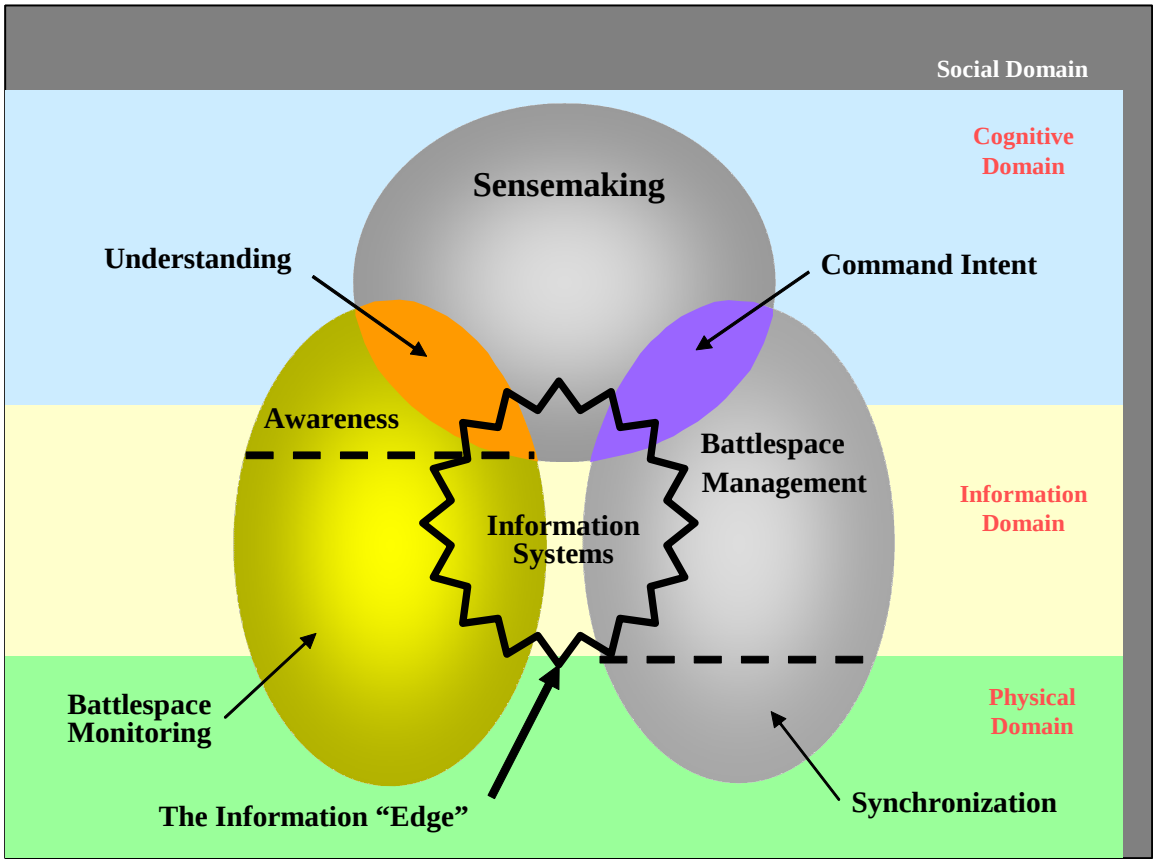

Figure 4: Elements of Command and Control

[8] David S. Alberts, Richard E. Hayes, "Power to the Edge: Command, Control in the Information Age", CCRP, June 2003, page 14-15.
[9] David S. Alberts, John J. Garstka, Richard E. Hayes, David A. Signori, "Understanding Information Age Warfare,", CCRP, August 2001, pages 142-3.

Given the C2 concept as depicted in Figure 4 (Elements of C2), one can make the following observations:

1) Platform-centric warfare predominately occurs in the physical domain;
2) Network-centric warfare predominately occurs in the physical domain with parts in the information domain;
3) Information-centric warfare predominately occurs in the information domain with parts in the cognitive domain; and,
4) Knowledge-centric warfare predominately occurs in the cognitive domain

One can view network centric warfare as the centerpiece of information centric warfare. Figure 5 below is a graphical representation of NCW within an information centric framework.

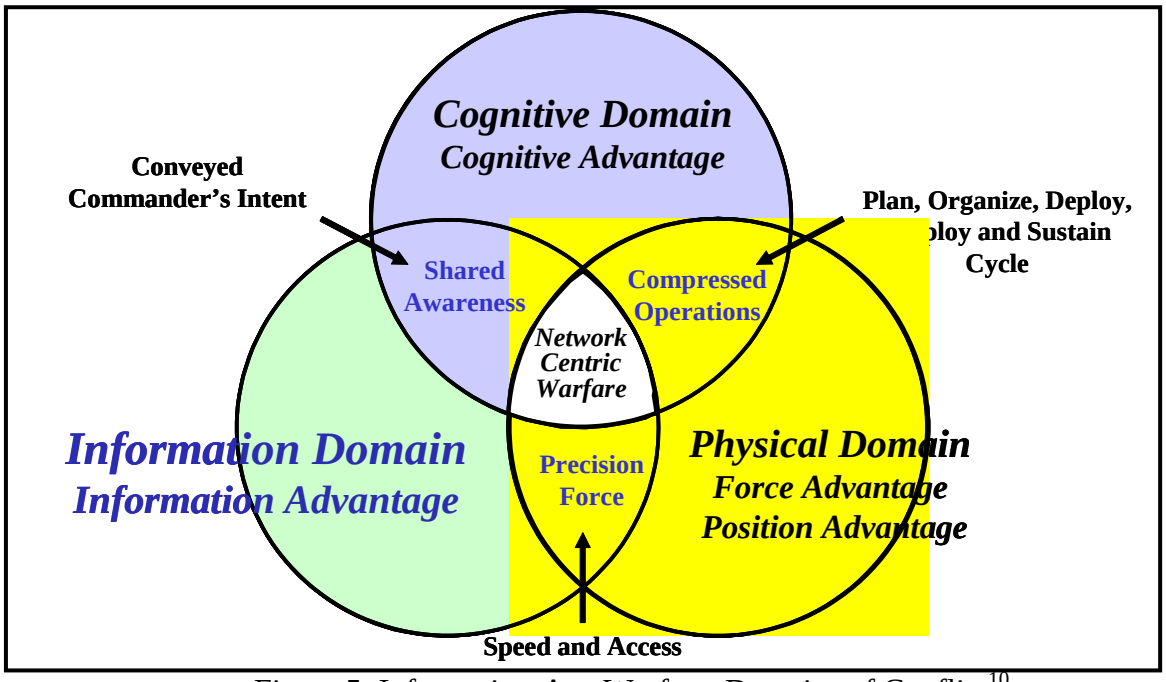

Figure 5: Information-Age Warfare: Domains of Conflict[10]

This graphic is used to illustrate that NCW is really part of information centric warfare.

[10] Briefing by John J. Garstka, LtCol Chuck Pattillo, "A Conceptual Framework for Network Centric Operations: Network Centric Warfare Europe," 4 Jun 2003

Knowledge Centric Warfare

Figure 6 illustrates an alternate view of the transition from platform-centric to network-centric, to information-centric to knowledge-centric warfare as we move further into the 21st Century, from a warfighters perspective.

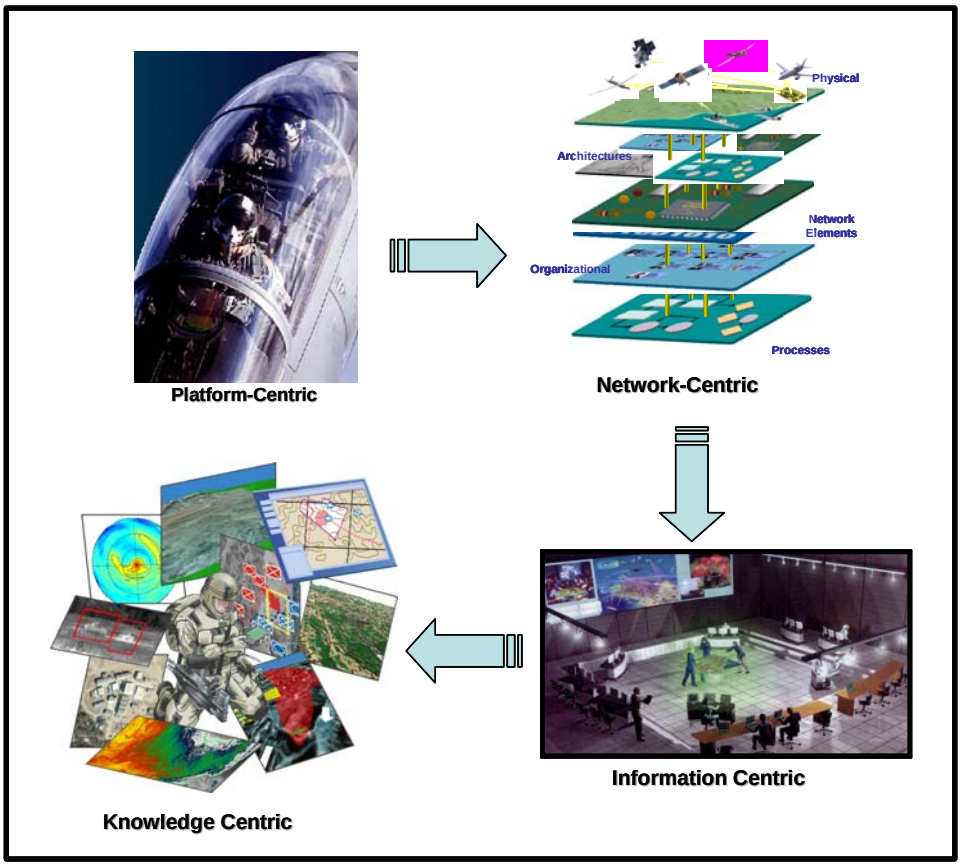

Figure 6: Transition from Platform to Knowledge Centric Warfare

First there was platform-centric (refer to Figure 5), where the B-17, the F-4 and the FB-111 were the "epicenter" of power. The pilot essentially determined the next course of action from the information presented at the morning briefing prior to the mission. The next logical step was network-centric warfare, where the B-2, the F-15 and the F-117 are all networked together. Given the state of the art in warfare, new constructs are possible that were not possible as little as 5-years ago, e.g., self-synchronization of forces. The next logical step in this evolution of warfare is information-centric warfare (some believe we have already started to enter this type warfare. In Operation Iraqi Freedom, where information was the force multiplier that allowed fewer troops to be used then many thought necessary). One can envision "information centers-of-gravity" where Commanders located in command posts (fixed and mobile) have the ability to assimilate and display vast amounts of fused data into useful forms of information to conduct the dynamic operations in the battlespace.

The step after information-centric warfare is knowledge-centric warfare, a further expansion of NCW. Taking the basic NCW constructs described earlier ("**Build** the net", "Protect the **net**", and "**Populate** the net."), in knowledge-centric warfare:

a. "**Build** the net" becomes "**Use** the net". Today's battlestaff has the capability to "surf the net" using information fusion engines, information pedigree, shared awareness, metrics, and information on demand. The end result is that instead of "building the net" as the center of gravity, the warfighter's use of the network becomes the center of gravity for the network, since some individuals/nodes will be more adept than others. This is, in essence, a transfer from a "physical" network to a "mental" usage of the network, i.e., knowledge centers-of-gravity.

b. "Protect the **net**" becomes "Protect the **knowledge**". Today's battlespace is centered on protecting the various networks from adversarial attacks. Within NCW this is information assurance and information operations. However, in knowledge-centric warfare, it's the "pockets" of knowledge that has to be protected from an adversary. Here adversarial intelligent agents would want to traverse the network seeking knowledge and having the ability to pass the knowledge back. New techniques will have to be developed in order to be able to protect the knowledge that will be pervasive on the network.

c. "**Populate** the net" becomes "**Know** the net". Today's internet is a good example of "populating" the net with users. This is the primary goal of on-line providers such as AOL and JUNO. However, in knowledge-centric warfare, the goal is to be able to "know" the what/where/when/why types of items. A good "surfer" using search engines available from yahoo™ and google™ will "know" the net to the point that when they need something they will know exactly where to go to get it (bypassing the search engines). In essence, they "know" the net.

The end goal of "Power **to** the Edge" becomes "Power **of** the Edge". The shift is from sharing information to sharing knowledge. Essentially "self-synchronization" becomes "virtual synchronization" to provide knowledge on demand, knowledge centers-of-gravity, and virtual awareness to the Commander and staff.

Alberts and Hayes, in "Power of the Edge", provide some insight into the ideas of Pigeau and McCann[11] who made the case for moving from a concept of command that is tied to an individual commander to a concept of command that is widely distributed. This idea of distributed command was introduced in *Command Arrangements for Peace Operations*. When battlespace knowledge is pushed to the outer edge along with the concept of distributed command, the end result is "Power **of** the Edge" in executing mission objectives.

This process has already started: new Army slogan is an "Army of one". This is an example of where knowledge is pushed to the lowest common denominator. It is a good example of knowledge enrichment that is, by design, scalable knowledge. The infantry soldier would have knowledge of the battlespace up to the Brigade or Corps level, but would have only cursory

[11] Alberts, David S., Hayes, Richard E., "Power to the Edge: Command, Control in the Information Age", CCRP, June 2003, page 18.

knowledge of what was happening in other battlespace theaters. This knowledge would change depending on the dynamics of the battlespace. One might draw the corollary to NCW of "self-synchronizing" forces to "self-synchronizing" knowledge. There exists a level of knowledge where the individual would be aware of this knowledge only when it rises (or peaks) above a certain threshold level.

The Navy's FORCEnet's[12] use of the "knowledge wall" is a good example of utilizing the attributes of network centric operations to "push" knowledge to a lower echelon. In this case, knowledge is pushed down to the carrier battle group into a "knowledge web" where warfighters have access to web pages, chat rooms for on-line discussions and reporting According to Rear Admiral Xelibor "…queries from higher echelons fell off…radio reports decreased significantly…redundant reports up, down and across the organization were virtually eliminated". FORCEnet will help transform how the Navy operates globally. The fleet will be able to reach back anywhere within the shore establishment and get more responsive support as entities farther down the echelon chain will become more self-sufficient and "knowledgeable" of the global situation.

Within NCW, there is the concept of publish/subscribe that assists the battlestaff. Essentially, information is provided on the net (published) so that all users of the net can receive the information (subscribe). Under a knowledge-centric concept, this changes somewhat. Information is still published but there is another level of data on the network for use by subscribers. That is, knowledge is published. Whenever the infantry soldier "figures something out", he can publish this knowledge, which may be useful somewhere else.

For example, if a soldier found a small device when searching a house in southern Iraq, he/she could, after analysis, publish on the net the following "knowledge": "Small detonator device with Afghan markings xxx". Another soldier in northern Iraq finds a fuse and publishes the following on the net "Fuse of type aaa found with Afghan markings yyy". Now, a third soldier (subscriber) stationed in Afghanistan is provided these small "tidbits" of knowledge. Taking this, the soldier combines it with what he/she knows locally and determines that there is a bomb making factory in a small Afghan town just 2-Kms down the road. His/Her squad investigates and finds the factory in the basement of the third house on the left. This is an example of collaboration of individuals heretofore un-connected. But by sharing information of the battlespace they are able to combine it into knowledge for action.

The armed forces are not as far away from thinking in terms of "knowledge-centric" warfare as one might think. For example, the British military use a command concept called "mission command", which is essentially "…a philosophy of decentralized command based on trust and initiative. Storr states that the key elements are: … timely decision making, the importance of understanding the superior commander's intention and, by applying this to one's own actions, and a clear responsibility to fulfill that intention…"[13] Storr further states "…the superior trusts

[12] Zelibor, Rear Adm Thomas E., "FORCEnet is Navy's Future." ISR Journal, Jan-Feb 2004, Vol3, No. 1, pages 18-20.

[13] Storr, Jim, "A Command Philosophy for the Information Age: The Continuing Relevance of Mission Command", "The Big Issue: Command and Control in the Information Age", Number 45, Strategic and Combat Studies Institute, Reprinted by CCRP, Feb 2003, pages 77-94.

his subordinate to act; to act within the commander's intent; and to act sensibly in the circumstances he finds himself, which are not necessarily those the superior envisaged when composing his orders…"[14] This philosophy lends very well to knowledge-centric operations since the knowledge to act is pushed down to the lowest level in the chain-of-command.

We have moved into a new generation of warfare, in which "knowledge-centric" will be the key to success. Russell states "…society's conditions are now in place for a change to a new generation, the 4th, of warfare (1st – massed manpower, 2nd – massed firepower, 3rd – maneuver) called "Netwar" in which antagonists will fight in the political, economic, social and military arenas and communicate their messages through a combination of networks and mass media…warfare will not be the relatively clear-cut, high technology 'stately dance' of conventional war but rather extremely complex, mainly low-intensity conflicts…[15]," The key to effectively addressing this new generation is to shift to "knowledge centers of gravity" where the military commander needs to not only know the military situation but the social, political and economic situation of the area under his/her responsibility. This new commander must have a "knowledge" base in order to effectively conduct operations not only in the present, but must be able to "predict" the next set of moves of the adversary to effectively achieve victory on the battlefield.

In a "platform-centric" environment the determinant is to ensure that the platform being procured is the best possible (F-15, F-16, F-22, JSF). In a "network-centric" environment, the primary consideration becomes acquiring "network-ready platforms" that can be networked with weapons and sensors and C2 nodes. By being part of the network, the platform is more effective than an absolute, individually independent, number would provide.[16]

Taking the logical extension, "information-centric" environment the determinant is to ensure that the information being "generated and circulated" is the best, most accurate possible. The last step, "knowledge-centric" environment the determinant is to ensure that the highest possible "knowledge" down to the lowest possible echelon is the best, and is as clear and accurate as possible.

Muellner states the battlefield of 2030 is where "…The determinants of success…will not be aircraft, ships or tanks, but rather, the exploitation of knowledge and speed of execution based on that knowledge…"[17] Furthermore, Muellner indicates that this new CONOPs will rapidly and decisively exploit superior knowledge of the battlefield, the enemy and "home" forces to prosecute attacks against the enemy at the tactical, operational and strategic levels in near-simultaneous fashion." Additionally, Muellner indicates that "… future warfare will be

[14] Ibid.
[15] Russell, John, "Asymmetric Warfare", "The Big Issue: Command and Control in the Information Age", Number 45, Strategic and Combat Studies Institute, Reprinted by CCRP, Feb 2003, pages 243-265.
[16] Potts, David and Thackray, Jake, "No Revolutions Please, We're British,", "The Big Issue: Command and Control in the Information Age", Number 45, Strategic and Combat Studies Institute, Reprinted by CCRP, Feb 2003, pages 29-42.
[17] Muellner, George, "Interoperability of a myriad of emerging broadband capabilities will become key", Aviation Week & Space Technology, December 15, 2003

dominated by the control of information. Properly exploited, information produces knowledge--of the environment, the enemy and home forces. Thus, gaining and maintaining information superiority will be an imperative.[18] Muellner goes on to say, "…To dominate the future battlefield, the information domain must also be dominated. Multi-phenomenological information must be collected, processed into useful knowledge and rapidly disseminated to decision-makers who can utilize it to shape and influence the combat sphere. At the same time, adversaries must be denied this capability….The second major determinant of success on the future battlefield will be the ability to produce decisive effects quickly. Speed of execution requires being able to project influence in all three dimensions on a battlefield rapidly…The technologies to enable this type of warfare are also becoming available. Knowledge creation will be aided by: improvements in information processing and storage; intelligent agents and decision-aiding software; digitally reprogrammable communication devices and broadband (including laser) communication links; persistent, survivable unmanned ISR vehicles, responsive, reusable launch vehicles that could deploy micro- or nano-satellites and stealthy interceptors to attack or defend high-value sensor systems..."[19] Lastly, Muellner indicates that "…These emergent technologies can be harnessed to create a new way of war--a concept of operations where superior knowledge is exploited with speed of execution inside an adversaries' decision/action cycle. Naturally, on the battlefield, things are dramatically different. There will be no defined lines of troops or forward or rear areas. Dispersed, knowledge-enabled entities conduct near-simultaneous, synchronized engagements across the battlespace. Each entity has common, shared battlespace awareness and seamless interoperability with the other systems. This network-enabled force can therefore collaborate to achieve a synchronization of force application and speed of command that maximizes its effect on the battlefield. Ground forces are inserted at the appropriate location, achieve their desired effects and are withdrawn quickly. Upon insertion, these forces are supported by a self-forming "task force" of resources. Knowledge and battlespace awareness are provided by the network. Fire support for these ground forces may come from an "arsenal aircraft" overhead, a ship offshore or a remote battery. Joint and coalition operations will require seamless interoperability between the land, sea and aerospace forces. This interoperability demands not only shared information and battlespace awareness but also interdependence in the application of maneuver and precision engagement on the battlefield. A command and control and decision-making environment will need to exist to allow commanders to execute dynamic planning and maintain full battlespace awareness at very high levels of operational tempo. All entities will continually report their system health and logistics state. Re-supply and other logistics support will be autonomic and largely supported from outside the theater to reduce theater footprint. Thus, the battles of 2030 will be fought on the ground and at sea as well as in air, space and information networks that support an adversary's way of life. Engagement in all of these domains will be necessary. It is this

[18] Muellner, George, "Interoperability of a myriad of emerging broadband capabilities will become key", Aviation Week & Space Technology, December 15, 2003

[19] Muellner, George, "Interoperability of a myriad of emerging broadband capabilities will become key", Aviation Week & Space Technology, December 15, 2003

simultaneous, theater-wide engagement across the tactical, operational and strategic levels that will characterize warfare…."[20]

Key Technology Areas of Knowledge-centric Warfare

Technologies that will support knowledge-centric warfare are those that deal primarily within the cognitive domain and upper levels of sensemaking (refer to Figure 4). Some of the more prominent technologies would be as follows:

a. *Publish / Subscribe / Broker:* Commanders, warfighters, and other combatants need an information management and exchange capability that supports tailorable, dynamic, and timely access to all required information to enable real-time planning, control, and execution of the aerospace mission. The Joint Battlespace Infosphere (JBI) will provide this capability. The essence of the JBI is a globally interoperable "information space" that aggregates, integrates, fuses, and intelligently disseminates relevant battlespace information to support effective decision-making. The JBI is part of a global combat information management system, established to provide individual users with information tailored to their specific functional responsibilities. It integrates data from a wide variety of sources, aggregates this information and distributes it in the appropriate form and level of detail required by users at all levels.[21]

b. *Predictive Battlespace Awareness*: Key to any engagement of an adversary is to be able to predict their next series of moves. This prediction, known as predictive battlespace awareness, contains a host of required technologies. Examples of these technologies are: a) real-time assessment of adversarial intent (the ability to predict what an adversary is planning to do so that Courses of Actions (COA) can be developed to stop and/or deter an adversary from taking the action predicted: this is an indicator to the planning process that steps will need to be taken to deter an adversary); b) decision theory (used for predicting human behavior in interactive situations. By relaxing the classical assumptions of perfect rationality and perfect foresight, we obtain much improved explanations of initial decisions, dynamic patterns of learning and adjustment, and steady- state distributions - such technology would greatly improve the anticipation of adversary actions); and, c) real-time Bayesian inferencing which provides a different approach to the estimation of adversarial response based on probabilistic reasoning.

c. *Effects-based Operations*: Planning in order to achieve desired outcomes (or effects) is at the heart of effects-based operations. Some of the related technologies are: advanced planning and scheduling techniques for future integrated command and control (C2) systems. These systems will employ planning and decision aid technologies to support a commander's exercise of command and control over forces across the full spectrum of military operations. The Information Directorate's research and development activities in planning, C2 decision aids, and integrated C2 systems will provide technology and processes to assist warfighters to dynamically

---

[20] Muellner, George, "Interoperability of a myriad of emerging broadband capabilities will become key", Aviation Week & Space Technology, December 15, 2003

[21] Phister, Paul W. Jr., Metzger, Richard C., Plonisch, Igor G., "Information Management for Space Situational Awareness: The Space Awareness Infosphere", AIAA-2003-2685, AIAA International Sir and Space Symposium and Exposition, July 2003.

synchronize force operations by collaborative execution monitoring and retasking of shared assets across echelons, missions, components, and coalition forces. Both national-level decision makers and warfighters will be provided with a proactive planning process with the ability to rapidly fuse and assess data and generate options and alternatives. Decision makers will assess crisis or combat situations more accurately and rapidly; develop multiple, high-quality response options; present the situation and options for decision; and rapidly plan in near real-time the allocation and assignment of resources.

d. *Distributed decision making capability:* This deals with collaboration and work flow management and how humans, machines and human/machine interfaces will work together to achieve the commander's intent. It covers the entire spectrum from telephones (human to human) to software agents which emphasize autonomy and cooperation (with other agents) in order to perform tasks for the user. Work flow deals with monitoring all processes (e.g. planning, scheduling, and COA analysis) and the ability to adapt timely solutions to problems. Furthermore, it will have the ability to inform the user on the status of the activity and expected time to completion.

e. *Cognitive reasoning*: This area deals with human interaction in complex automated systems and the need to apply cognitive engineering principles in developing a more effective and efficient human-technology system. It strives to understand the cognitive skills underlying behavior such as problem solving, decision making, and assessment and applies that knowledge to the benefit of human-technology systems. Cognitive reasoning deals with the understanding human-technology interactions with the goal of developing information systems to support improved human performance. It treats human cognitive abilities explicitly to assure information is provided to the user in a meaningful way. Advanced human system and cognitive skills are an approach to understanding human-technology interactions.

f. *Behavioral modeling:* Neurobiological modeling involves the study of how the human brain functions, reasons and assesses data, information and knowledge. The understanding of this process can then be mimicked in machines which can give more human-like alternatives for a decision maker to consider. Analysis interdependencies and emergent behaviors of complex adaptive systems involves simulations of multiple, interdependent infrastructures. It includes research into interdependencies and emergent behaviors of complex adaptive systems. Adversarial culture modeling is a major challenge to modeling, simulation, and/or analysis involving diverse cultures among participants (allies, coalitions, and adversaries). The inability to understand and predict the behavior of individuals and groups when fundamental societal assumptions are different from one's own is a key C2 issue. This research element addresses the problem of modeling and predicting the behavior and interactions of cooperating, and, more significantly, competing cultural representatives. Future military operations will depend on the effective management of coalitions composed of partners who share only temporary interests. This can be considered to be a special case of adversarial culture modeling.

g. *Advanced simulations (helmet, "holodeck"):* A key C2 capability is the interface between the machine and the human decision maker. Visualization technologies required include: a) advanced immersive multi-sensory interfaces to connect man and machine together so that decisions can be made synergistically, faster and better; b) human/machine interaction

(visual, sound, tactile) to understand human-technology interactions with the goal of developing information systems to support improved human performance; c) human interaction in complex automated systems to apply cognitive engineering principles in developing a more effective and efficient human-technology system; and, d) virtual reality "killer apps" that will allow the warfighter to perform critical tasks faster or in new ways using totally immersive display technologies.

As a result of the integration of these technologies, the result will be "Virtual Command Centers," which are the Commanders' means of locating, assembling, directing, and coordinating the efforts of a battle staff that is geographically distributed but virtually centralized. If required by events, it allows an ad hoc staff to be assembled and be fully operational in only seconds, and then disbanded. It permits tighter connections among the entire warfighter team, including the ability to more positively control weapons assets; and virtual beings. The process of virtual command will be augmented by virtual beings who encapsulate the behavior of a trusted expert for the purpose of providing information or executing a task. The warfighting commander would interact with virtual beings in a natural manner, through natural language, to project and extend the effects of the commander's intent and direction.

h. *Knowledge Reasoning:* Within the knowledge domain, the required technologies are: knowledge discovery and machine learning, where the need to develop automated capability to reason, infer and discover knowledge implicit in extracted information**.** Knowledge Discovery applies to developing technologies that automatically present humans with enhanced information formulations and tools that aid in the formation of a mental picture that leads to the discovery of new knowledge. Knowledge Discovery technology deals with machine learning, case-based reasoning, similarity metrics and pattern learning. Data Mining and Text Mining are subsets of Knowledge Discovery, which deal with visualization of fused information from multiple sources, information relationships, and pattern variations. There exists a need to develop the necessary machine learning technologies to enable a system to learn, from example instances consisting of data about entities, relationships, and their attributes, and models of scenarios of interest. These technologies would likely include pattern representations and languages, as well as algorithms for learning patterns represented in these languages. They would also include data representations that will provide scalability with respect to pattern size and complexity, as well as with respect to the vast amounts of available data. Researchers have begun to explore promising new techniques for relational classification and for learning probabilistic relational models. Other techniques from areas such as inductive and stochastic logic programming can represent the complexity of the relationships, but have not been exercised on data sets anywhere near the required size. Approaches such as learning with prior knowledge, active learning, and incremental and cumulative learning may be useful.

i. *Intelligent Agents:* The development of intelligent dynamic software agents will be important. These software agents will need to be self-learning and autonomous in order to have the ability to gather and provide needed information/knowledge from other sources in time to impact the information/knowledge provided to a decision maker.

j. *Modeling & Simulation:* This area will need to cover perturbation theory. Tasking can be viewed as the formulation of a trajectory through state space and retasking as a perturbation to the original task. Research in this area may significantly reduce the computational complexity inherent in brute force solutions. It also needs to cover decision theory. A key area within modeling and simulations is that of COA analysis. Key technologies include:

a) Pattern-based 'behavior' M&S of the decision maker. This connects decision-making pattern based behaviors (desired political-military outcomes at the operational and strategic levels) to specific physical effects (operations and military actions). This interdisciplinary research includes political sciences, social networks, human interactions with technology and infrastructures, bureaucratic mechanisms and policies, and legal/policy/regulatory structures;

b) Real-time updating of simulations. This includes real-time data ingestion and updating, dating mining, data validation, and methods of handling extremely large, dynamic datasets. This research will enable the incorporation -- in real time -- of the results of attacks on enemy assets into dynamic EBO planning tools and decision aids; and,

c) Self-organized modeling of interdependent (military, economic, social, etc.) infrastructures and 'emergent' behaviors of complex adaptive systems. This basic ability will have models automatically organize themselves based on present and predicted battlespace environments.

Another key area within modeling and simulation deals with the socio-economic modeling of organizations and nation-states. Key technologies here are socio-political network analysis and prediction tools. Lacking today are tools which accurately model the socio-political nature of a culture, nation, or terrorist organization. Having the ability to predetermine how an adversary would react to an action taken is crucial to the development of predictive modeling tools. Also, having an understanding of the socio-political dynamics internal to a group or organization may allow for actions other than war to diffuse the adverse intent of the group.

k. *Multi-domain information fusion:* New fusion approaches are needed to reduce information ambiguity from multiple sensor types and geo-locations to include ground, air & space.

l. *Knowledge pedigree/information assurance*: In order to provide accurate information/knowledge to a decision maker, one must know that the information/knowledge is "good" and valid. Research in determining the validity of information/knowledge and to be able to determine whether the information/knowledge has been tampered with, is essential. Also needed is assurance that the information is from a valid source and has not been compromised.

m. *Self-learning Knowledge Extraction:* This is the development of an automated capability to reason, infer and discover knowledge implicit in extracted information. Knowledge Discovery applies to developing technologies that automatically present humans with enhanced information formulations and tools that aid in the formation of a mental picture that leads to the

discovery of new knowledge. Knowledge Discovery technology deals with machine learning, case-based reasoning, similarity metrics and pattern learning. Data Mining and Text Mining are subsets of Knowledge Discovery, which deals with visualization of fused information from multiple sources, information relationships, and pattern variations. There exists a need to develop the necessary machine learning technologies to enable a system to learn from example instances consisting of data about entities, relationships and their attributes, and models of scenarios of interest. These technologies would likely include pattern representations and languages, as well as algorithms for learning patterns represented in these languages. They would also include data representations that will provide scalability with respect to pattern size and complexity as well as with respect to the vast amounts of available data. Researchers have begun to explore promising new techniques for relational classification and for learning probabilistic relational models. Other techniques from areas such as inductive and stochastic logic programming can represent the complexity of the relationships, but have not been exercised on data sets anywhere near the required size. Approaches such as learning with prior knowledge, active learning, and incremental and cumulative learning may be useful.

Summary

This paper is intended to look beyond network-centric warfare to the next possible step in the evolution of warfare. This next step is a move from the predominately physical (Network-centric) to one of more mental (knowledge-centric) level warfare. Taking the basic Network-Centric Warfare constructs described earlier, knowledge-centric warfare transforms the emphasis as follows: a) "**Build** the net" becomes "**Use** the net;" b) "Protect the **net**" becomes "Protect the **knowledge;**" and, c) "**Populate** the net" becomes "**Know** the net."

Acknowledgements

Special thanks go to Kyle Holbritter and Anna Lemaire for their time and effort reading this paper for content consistency.

Bibliography

Paul W. Phister, Jr., Ph.D., P.E.
Paul Phister is the Air & Space Strategic Planner at the Air Force Research Laboratory's *Information Directorate* headquartered in Rome, New York. Dr. Phister holds two masters degrees and received his Ph.D. in Engineering from California Coast University. Dr. Phister is a licensed Professional Software Engineer from the State of Texas.

Igor G. Plonisch
Igor G. Plonisch is the Chief of the Strategic Planning and Business Operations Division at the Air Force Research Laboratory's *Information Directorate* headquartered in Rome, New York.