Making NCW a Reality

Clearly, NCW has significant potential to transform our approach to assigned missions and achieve worthwhile improvements in effectiveness and efficiency. However, these gains will not be realized by simply putting an enabling infostructure in place. In fact, doing so without taking decisive steps to develop NCW-based mission capability packages could result in confusion and disharmonies, along with degraded performance and poor morale. Making NCW a reality requires that we first start with a clean sheet of paper and understand the implications for all of the elements or components of the force.

Two key prerequisites for success are in our control:

1) the development of new and innovative NCW concepts and strategies to meet mission challenges; and
2) the ability to transform these embryonic concepts and strategies into real operational capability, unconstrained by current institutional considerations.

What is needed to accomplish this are three linked processes—one designed to foster and incubate innovative ideas, one designed to introduce change, and a third process designed to insert technology. History is replete with examples of organizational failures to take timely advantage of the opportunities that advances in technology afford. These opportunity losses usually can be traced to a failure of (or lack of) one or more of these processes or the absence of the necessary links among them. History demonstrates that progress is eventually made, albeit at a much slower pace than was possible. Before the relatively recent explosion in the pace of technological advances, usually new technology was assimilated before it was itself obsolete. Technology is now advancing at a rate which far outpaces our ability to fully leverage its potential, and it is not uncommon to have organizations operating with technology that is more than one generation removed from the cutting edge. In fact, large organizations like DoD deploy at any given time technology from several different "generations." This only exacerbates problems with interoperability and security.

The Information Age is different, particularly for the military, than past eras in four fundamental ways that makes "business as usual" increasingly obsolete. First, the rate of technological advance, and the ability to turn out new products, has increased dramatically. Second, the advances in technology that are relevant for the military are, to a very large extent, no longer driven by known operational requirements.[102] Instead, they are being driven by private sector requirements to move and process information on a scale unimaginable just a few years ago. Third, the military is now being driven by a technology cycle that is quickening and has less and less time to react to take advantage of the new capabilities they represent before these, in turn, are overtaken by new capabilities. Fourth, the new capabilities are equally available to potential adversaries.

While much has been learned about putting technology to use, the pace of technological advances has quickened to such a degree that current DoD methods of incorporating technology are well behind the power curve. While reforms are underway to help reduce the time it takes to go from design to deployment, they alone will not be sufficient to bring about the changes needed to meet today's mission challenges. The reason is that the technology development cycle is out of sync with military strategy and doctrine development. Speeding up the technology cycle, without addressing the inertia in the processes by which we develop military strategy, concepts, and doctrine, just makes these processes more out of sync. What is needed is an approach that synchronizes the development of military strategy and doctrine with the advances in technology and with the technology insertion process.

The speed at which technology can be deployed is only one aspect of the problem. Consider a situation in which new technology can be made instantly available to operational users. How much of the technology's potential will be realized? At best, only incremental improvements will be made and only a small fraction of the potential utility of the technology will be realized. This is not to say that these incremental improvements would not be useful, or even important. But inescapably, a great deal of the potential of the technology would be unrealized. This scenario would be repeated over and over again as the latest technology replaced older technology. Thus, only a series of incremental changes and improvements in operational capability would be achieved.

What is needed is a set of tightly coupled processes that:

1) facilitates an understanding of emerging capabilities;
2) fosters innovative concepts;
3) expedites the testing and refinement of these concepts; and
4) focuses efforts on the development and deployment of coherent MCPs.

To achieve this we will need to adapt our existing requirements, investment planning, and programmatic processes, making them enterprise-wide in order to make NCW a reality in a timely fashion. Current practices bifurcate the requirements, funding, design, development, and acquisition processes for each of the elements of an MCP. Thus, rather than helping us coevolve, our culture and processes are doing just the opposite.

Lessons Learned

One can trace the origins of our current understanding of the need to coevolve MCPs to earlier work in evolution acquisition by the DoD and industry.[103] The rapid prototyping component of evolutionary acquisition[104] (EA) foreshadowed the current notion of coevolution. The concept of EA was developed as a result of widespread dissatisfaction with the results of systems acquisitions. More often than not, systems were delivered late, with significant cost overruns and worse of all, they failed to satisfy users even when they delivered the specified functionality. Before EA, systems were designed and acquired using a waterfall approach that moved sequentially from step to step, beginning by specifying the requirements in considerable detail. Once these requirements were specified and approved by the operational community, they were frozen, and developers went off to produce a system (taking a decade or so before it was returned as a fait accompli), and then finally it was turned over to the users (who of course were not the same ones who participated in the requirements phase). We, of course, know better now. But then systems were just beginning to be software dominated and the flexibility of software vis-à-vis hardware was not widely understood. But it is instructive to see what the developers of the EA approach identified as critical back then and note in their observations and recommendations the origins of our current philosophy of coevolution because it provides us with a better understanding of what will happen if we do not insist upon processes that will encourage and facilitate coevolution of MCPs.

Prior to EA, there was a commonly held belief that most of the problems incurred in systems development could be traced to poorly articulated requirements, and if only the users would just do a better job writing document requirements, everything would be fine. But the founders of EA recognized that users, no matter how hard they tried, were unable to specify in advance all of their requirements. This inability was not found to be caused by a lack of effort devoted to the requirements process, as was previously thought. Instead it was the result of a faulty assumption. It was believed that users know what their requirements are, or at least *should* know. In fact, it is unreasonable to expect users to know, in any detail, what their requirements are or will be, when they do not have a full appreciation of the new or improved technologies, particularly in terms of implications for the environment or mission.

Traditionally, users first saw technologies after they were packaged into deployable systems. Only after users gained experience with the new capabilities were they in a position to fully appreciate the possibilities in the context of their jobs. There are many problems associated with the dump-technology-on-the-users-and-run approach. First, the learning curve was often steep and it took some time before a significant portion of the new capabilities was actually employed. Second, only a fraction of the features contained in a system found their way into widespread use. Third, it was only after users started to appreciate the new technologies that they were able to think of ways they could be used. Let us look at each of these problems and see how EA was designed to remedy them so that we can incorporate these lessons learned into our approach to developing applications of NCW.

It turned out that the learning curve was more complex than originally thought. While much attention was focused on training users to operate the system to become familiar with the "knobs and switches," it soon became clear that command and control systems were not to be mastered simply by learning the user interface. In many cases the information contained in the system was significantly different from the information that was previously available. It may have been entirely new, a class of information that users only dreamed about having before, or sometimes information they never even knew existed. It may have been the same information except that it was now more timely or accurate. The information characteristics may not have changed, but the way information is presented could change. Finally, it may have been new analytical capabilities that took available information and added value to it.

In these cases, learning the system involved much more than learning the user interface. It took (and takes) time and lots of on-the-job practice. And the learning did not end there. Once a new capability was mastered and confidence was developed in its reliability, users started to see the possibilities. And these possibilities involved learning curves of their own. In fact, this was the hidden set of learning curves that EA brought out into the light. These "extra" learning curves were, in fact, users learning their new requirements. In retrospect, it seems ludicrous to have thought users could capture their requirements in a document without ever having been exposed to a hands-on version of the system in question, or without a chance to use the system in an operational context.

As a result of this improved understanding of the extent of learning that needs to take place, the EA approach scrapped the lengthy and unproductive paper requirements process and replaced it with the use of rapid prototypes, or simulations, that give users an approximation of hands-on experience. It uses the statement of requirements that is implicit in the iteratively developed prototype as the true expression of requirements. The EA approach speeds up the learning curve and matures the requirements more rapidly than before.

This lesson, once learned, needs to be relearned. In most if not all of the experiments to date, there simply has not been enough time provided to allow users to learn what the new systems could do and as a result the experiments are not as productive as they could be otherwise.[105]

The second problem with the traditional approach was that only a fraction of the systems capabilities was ever fully used. The causes for this vary widely. They include:

1) poorly conceived and/or executed requirements;
2) potentially very useful capabilities that cannot reach their potential because of constraints imposed by doctrine or organization;
3) capabilities that require more training to understand and employ; and
4) a lack of user trust or confidence in the system.

Replacing the paper requirements process with an iterative, hands-on approach also helps to address some of the root causes for failures to use system capabilities, but is inadequate in addressing the existence of self-imposed constraints. The full recognition of this problem, and the development of an approach to deal with it, was not fully articulated until the development of the MCP approach and with it the recognition of the need for coevolution. While an improved requirements process alone can make a significant difference, other aspects of EA serve to reinforce it and improve the probability that a system's capabilities will be useful when delivered. The notion of not biting off the whole job at once, but rather developing a set of core capabilities as an initial deployable delivery, aids the cause by reducing the amount of learning that users need to do and the change they need to assimilate. It makes it easier to move up the learning curve and reach a level of improved productivity and effectiveness, contributing to better user acceptance and confidence in the system. This incremental, or gradual, approach to innovation and change has its limitations. The tendency has been to modify and improve (at times dramatically) existing processes, but rarely to create new processes that replace existing processes. The result is sub-optimal, and we may incur a huge opportunity cost, as discussed later on.

The third problem identified above involves the dynamic nature of requirements. It was a breakthrough of sorts to explicitly recognize and accept that requirements will change over time, not only as a result of changes in the environment (e.g., the threat) but as a result of learning. Rather than treating this phenomenon as a flaw in the design and acquisition process, and tagging it with the inglorious label of requirements creep or growth, EA recognized it for what is was—the result of an interactive adaptive process.

When users expressed dissatisfaction with systems that met or exceeded their original specifications, it was a frustrating experience all around. In an effort to keep costs down, developers froze the specifications and ended any effective interaction between developers and users. The rationale was that the developers would not be distracted from their complex task of building the system. While this had the intended effect of reducing the costs associated with development and time to deliver systems, the price that was paid in operational effectiveness and user alienation was very high. EA recognized that this approach was counter-productive, and replaced it with the build-a-little, test-a-little, field-a-little strategy, with emphasis on a close-working relationship between users and operators.

As we begin to develop NCW applications, we would be well advised to keep in mind two key facts of life (recognized by EA), and leverage rather than fight them. The first, as identified above, is the need for users to become better acquainted with technology and its possibilities before they can intelligently develop NCW concepts. The second is to understand that these concepts must be allowed to evolve over time. To help ensure success, we should incorporate the following key components of EA into the process by which we coevolve MCPs:

1) continuous user involvement;
2) use of rapid prototypes to allow users to get tangible representations of the future;
3) build-a-little, test-a-little philosophy; and
4) develop an architecture that accommodates the changes that will surely come.

Role of Experimentation

Different kinds of experimentation will be needed at various points in the coevolution of NCW. There are three basic kinds of experimentation.[106] These include experiments designed to discover better ways of doing things, to test hypotheses, and to demonstrate (or confirm) what we believe as laws or facts. The first of these, Discovery Experiments, essentially generate hypotheses that are subsequently tested by Testing Experiments and confirmed by Demonstration Experiments. All experiments include, to one degree or another, assessments about the potential operational utility of an MCP, or part of an MCP.

Three classes of hypotheses need rigorous developing and testing on the road to NCW. The first involves the nature of shared awareness and what it takes to achieve it. The second involves the nature of self-synchronization and its mission-related utility. The third class of hypotheses that need to be tested involve the relationships between shared awareness and self-synchronization.

Role of Experimentation in the Coevolution of MCPs, Figure 35, presents an overview of the process by which concepts for new MCPs could be conceived, tested and retested, and finally transformed into a real operational capability. To achieve its goal, the MCP process focuses, synchronizes, and coordinates the efforts of numerous DoD organizations. Components of this MCP process currently exist, but the glue needed to hold these pieces together is weak, and the overall process itself is not as well

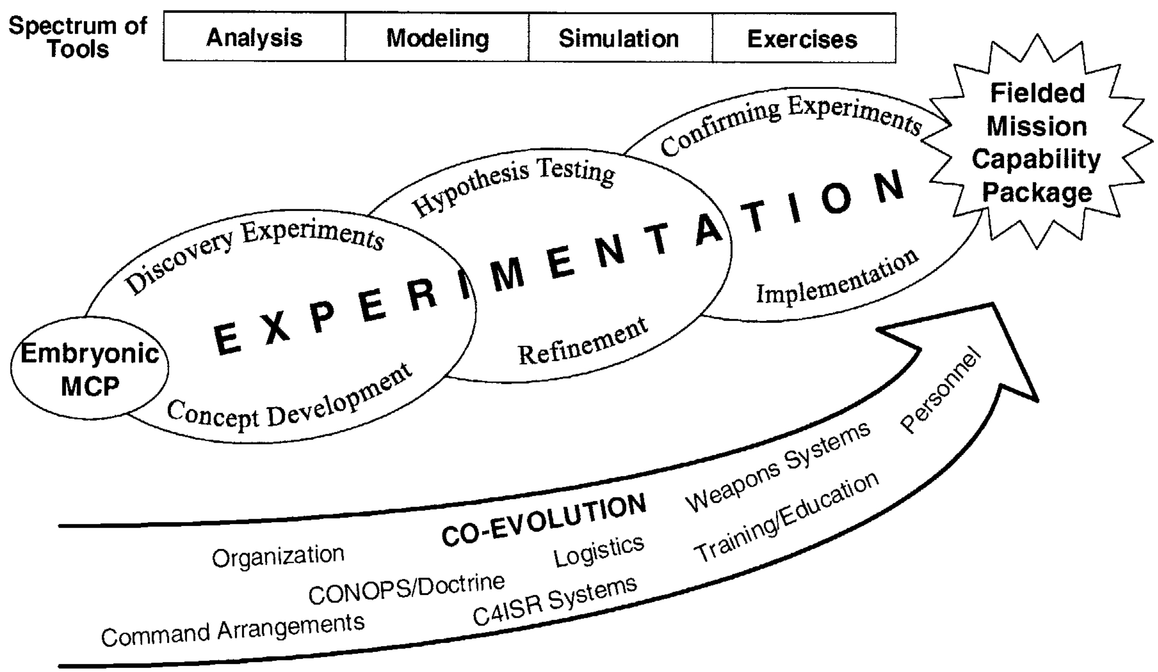

Figure 35. Role of Experimentation in the Coevolution of MCPs

focused as it could be. We currently are weakest in the front-end, or conceptual, phase and in accepting and implementing approaches that require changes in culture.

In the Concept Development Phase, groups of individuals, with the requisite operational and technical expertise, need to be brought together in a safe environment and with the charter to "think outside of the box." DoD needs to develop environments well suited to this task. Environments designed to facilitate innovation are expected to be an integral part of the process of Joint and Service Experimentation, and the designation of USJFCOM as the executive agent of Joint experimentation will help focus these efforts. While the need for experimentation is beginning to be widely accepted, there are different views on just what experimentation is all about. One size does not fit all as far as experimentation goes.

As concepts jell, they would be then subjected to a series of analyses, experiments, and tests to be refined to determine if they merit adoption by the DoD. It is essential to keep users heavily involved, insuring that each aspect of the package: command concepts and organization; doctrine and procedures; force packages; technology and systems; and training and education; is mutually supporting and operationally sound. The Concept Refinement Phase, having a distinctly hands-on flavor, is essential to facilitating effective communication among the communities.

DoD has invested in a full spectrum of models, simulations, testbeds, and instrumented ranges to support the testing of weapons, systems, equipment, doctrine, and concepts of operations for the training and exercising of our forces. While these valuable resources help to support the assessment and refinement of MCP concepts, several areas of weakness need to be addressed. Most urgently there is a need for explicit and flexible representation of command and control, and the effects associated with what has become known as information operations. While work needs to be done at all echelons of command, the most pressing need is at the CINC and JTF levels, with an emphasis on coalition operations. These models and simulations need to be able to accommodate changes in all aspects of the MCP, including doctrine, organizations, command approaches, lines of authority and information flows. Without this capability, these expensive investments will be unable to shed light on the critical issues being addressed by DoD. Equally obvious is that these models and tools no longer can be solely designed to support a particular segment of the community (e.g., training), but need to built with the idea that they will be used in all phases of the development of MCPs.

The last phase of the process requires the implementation of the institutional changes, technologies, and systems that are required by an MCP. At some point, a successful mission capability package concept will have gained sufficient credibility and the need for certain institutional changes will become widely recognized. This is a critical junction because it is here that the battle with the forces of inertia is joined. Given the knowledge of this battlefield in advance, it is important that the senior civilian and military leadership fully embrace the MCP process, and stay abreast of the development of MCP concepts and progress.

What is necessary is a mission-by-mission review of how we can meet the challenges we face. Since organizations need to continually accommodate change in the nature of their missions, the creation of structured "change processes" are required to facilitate and develop new MCP concepts and translate them into new operational capability.

Assessing the Potential of NCW

The DoD has a rich and diverse set of analytical tools and models that support analysis; unfortunately, few are suitable for the task of assessing the potential contributions of concepts, approaches, and systems based upon NCW. Many of our large detailed simulations were developed by and for the training community who were interested in developing and assessing competencies based upon current organizational structures and doctrine in the performance of tasks that contribute to traditional combat. These models are often hard wired for these purposes, and do not have the capability to reflect the very different set of assumptions, flow of information, or measures that are associated with NCW concepts of operations.

One reason that the analysis task is so challenging is the need to let more aspects of the problem vary. The application of NCW to a military situation or problem requires starting with a clean sheet of paper and designing a mission capability package from scratch, finding the most appropriate combination of a concept of operations, an approach to command and control, an organizational structure, a set of information flows, all to be matched with appropriate sensor and engagement capabilities. As we depart from the comfort of the status quo, we raise questions about expected performance that cannot be directly inferred from past experience. Warm and fuzzy feelings are unlikely to prove an acceptable substitute for solid analysis.

The key to any analysis (both its face validity and its utility) is the set of measures used to represent the performance and effectiveness of the alternatives being considered. We are relatively good at measuring the performance of sensors and actors, but less adept at measuring command and control. Command and control, to be fully understood, cannot be analyzed in isolation, but only in the context of the entire chain of events that close the sensor-to-actor loop. To make this even more challenging, we cannot isolate on one target or set of targets but need to consider the entire target set. Furthermore, NCW is not limited to attrition warfare, but is designed to support other concepts such as shock and awe. It is not sufficient to know how many targets were killed, but exactly which ones and when they were killed.

We have become better at characterizing the contribution of command and control as we have moved away from relying upon communications-focused measures like the probability of correct message receipt (PCMR) to targets at risk.[107] But we need to do more. Although using targets at risk is a great improvement in C4ISR analysis, it does not address a number of questions that are important for understanding NCW. The questions revolve around issues of battlespace awareness, planning, and execution. Targets at risk is a measure that combines aspects of each of these, but is essentially a measure of potential whose degree of realization is greatly dependent upon one or more aspects of an NCW-based approach to command and control, organizational, doctrine, training, and characteristics of the user interface (visualization). It is important for us to develop ways to characterize and reflect these attributes in our analyses and models.

Measures of Merit

One way to force the issue is to design a set of measures that focus our attention on these critical aspects of the problem. Some issues and questions that need to be explored to augment the targets at risk approach, and move it from a measure of potential to a measure of expectation, include:

1) Who in the battlespace is best equipped to make each firing decision?
2) Is the concept of operation, doctrine, organization, and training supportive of this?
3) How many decisions are expected to be needed, in what time frame, and to what extent is this feasible?
4) What is the impact of not allocating certain classes of decisions to specific individuals, but permitting overlaps (or gaps)?
5) Which decisions could be automated, and what is the best way to distribute the remaining decisions?
6) What information is most important to support time-critical decision making, and can it be made available to the individual responsible?

7) What is the impact of distributed teams sharing access to information and acting without prior synchronization?

The above questions illustrate the nature of the unknowns we need to explore if we are to make the most out of the opportunities afforded by the Information Age. To shed light on these issues, we will need empirical data and measures to guide our data collection and support analysis. This is why experimentation is critical to our efforts to transform NCW from a theory into practice.

At the heart of any assessment process are the measures of merit employed. In assessing the value of applying NCW to a variety of National Security missions and tasks, we will need to augment the measures we currently employ if we are to be able to better understand the impacts of NCW and the value of this new approach. It is one thing to adopt a new approach and compare the outcomes that result to a baseline case, and quite another to understand why different outcomes result. One might ask why this matters. What does our understanding buy us? After all, if we know that Approach B is better than Approach A, is this not enough? The answers to these questions lie in the complexity of applying NCW to military tasks. More information is not always better. More connectivity is not always better. More autonomy for actor entities is not always better. In many cases the response curve will increase for a while, then level off, and may at some point even go down. It is important to know the shape of these curves so we not only maximize mission-related measures, but also do so economically and efficiently. It will be important for us to know under what circumstances the MCP characteristics associated with NCW approach work and when they do not.

Currently, we think about five basic levels of measures (see Figure 36, Hierarchy of Measures). The first level involves measuring the performance of the C4ISR systems as federated into an infostructure, which is our computation power and ability to transmit or distribute information—connectivity and bandwidth. We have long recognized that increases in these measures do not *automatically* translate into increased mission success.

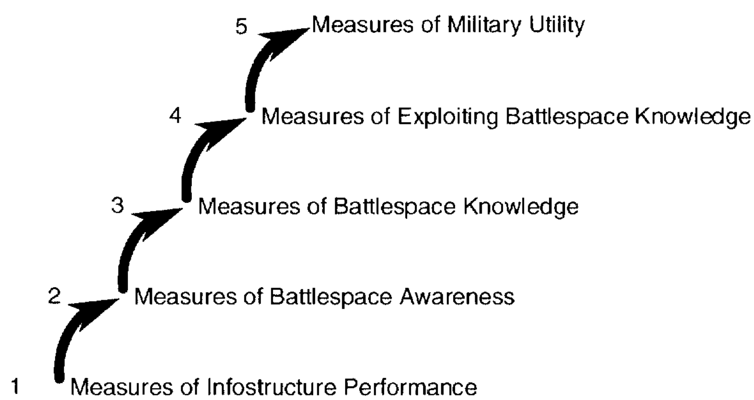

Figure 36. Hierarchy of Measures

At the other end of the measurement hierarchy, we have measures related directly to mission effectiveness or utility. For combat operations, common measures that have been employed have included attrition rates, FEBA movement, fratricide, leakage, and time to accomplish a given mission. In our opinion, we must continue to work to improve these because neither do they often tell the whole story,[108] nor are they applicable to many of the missions we find ourselves undertaking in the Information Age. For example, the U.S. Navy in its analysis of the impact of IT-21 added *speed of command* to the traditional measures of time to objective, losses, high priority kills, and assets utilized.[109] OSD Net Assessment is undertaking a study to identify and explore the most promising measures of effectiveness for NCW.[110]

The fifth level (utility) was needed because some mission-related measures were found to be highly dependent upon scenario-related factors, and it was important to consider the robustness of a particular improvement. This fifth level involved a set of measures that portrayed the robustness of the alternative as a function of the scenario space. Recently, some have advocated explicit consideration of a sixth level, Measures of Policy Effectiveness. This level would allow us to assess the contribution of a military operation that was part of a larger undertaking, such as Peace Operations. There may indeed be cases where "successful" military operations are not sufficient to achieve policy objectives. In these cases it is important to understand the limits of military power.

Given this measurement hierarchy, we could address the question of whether an MCP was better than a baseline case, and we would be able to identify the impact it had on each of these five levels. But if we did not develop a set of measures that reflected NCW-related characteristics of the MCP, we would be unable to generalize or leverage the experiment. Put another way, in a particular case we might find that an MCP resulted in better information quality, better decision quality, and improved mission effectiveness, but it would not be proper to conclude that better information alone resulted in better decisions, or that better decisions alone resulted in improved mission effectiveness. An NCW-based MCP could be expected to differ in any number of ways from a non-NCW-based MCP. For example, organizational effects could be a key factor. We need to be able to identify and measure key features of NCW, measure them, and relate these characteristics to the measurement hierarchy.

The identification of key aspects of NCW-based MCPs needs to be addressed by the analytical community in close cooperation with the operational community. In tackling this task, we should bring to bear the fine work of many scientists from a number of different disciplines, ranging from cognitive scientists and organizational theorists, to those who study complexity.

How well the components of an MCP are matched will be of concern. For example, is the division of tasks matched to the dissemination of information? Are the decisions being made at the best time by the most qualified decision entity? Is the available battlespace knowledge being leveraged? We will want answers to these questions and others as we travel on our journey to implement NCW concepts. In other words, we want more out of our analyses than "B was better than A." We want to understand why, so we can apply the lessons learned to develop the best NCW-based MCPs.

The Journey Ahead

We are embarking upon a journey of discovery. The end state of our warfighting force in 2010 and beyond will emerge through a process of experimentation. There will be failures along the way. We will find that ideas that seemed promising could not be translated into combat power. Our success will depend upon our collective will, the preparations we make, and how we are provisioned. In this concluding chapter, the major challenges faced are identified, for it is only by being well prepared to meet these challenges that the journey will be a fruitful one.

The most significant challenges to be faced include:

1) the development of a shared understanding of the nature of national security in the Information Age;
2) the ability to work in a coalition environment;
3) the achievement of true jointness;
4) the coevolution of NCW-enabled MCPs;
5) the development and implementation of an investment strategy that supports NCW-enabled MCPs; and
6) the development of an appropriately skilled, educated, and trained force.

Security in the Information Age

The United States, as the only superpower, has yet to find a comfortable role in a changed world. However, it is clear that our role and the threats we face will be different and require us to adjust our view of missions, tools, and ourselves. Defending the nation and its vital interests in the future will involve more of an emphasis on asymmetrical threats and the conduct of operations other than war. Changes both in the geopolitical situation and advancing technology are driving the changes taking place in the security environment. Changes in the geopolitical environment have also resulted in the need to undertake significant operations in coalition environments. The proliferation of rapid advances in technology has put powerful weapons in the hands of a host of players, greatly increasing their significance and potential threat.

These weapons include both weapons of mass destruction (WMD) and the tools associated with information warfare, and in its most troubling form, infrastructure warfare. In some instances, the lines between peace and war and the distinctions among friend, foe, and neutral are becoming blurred beyond recognition.

Asymmetric warfare presents a unique set of challenges, not the least of which include finding successful strategies for deterrence, detection, and response. Lethal responses may become of little value in many situations when their political costs far outweigh their effects. Asymmetric warfare involves each side playing by its own set of rules, determined by their respective strengths and attempts to exploit an adversary's weakness. It is a far cry from the tank-on-tank battles or naval engagements of the past. This makes it very difficult to develop indications and warnings normally used to see if someone is preparing for war. Rather than working around the clock to produce airplanes or WMD, an adversary may be educating computer scientists.

If we look at these changes as a whole, it is clear that our missions have gotten to be far more complex, and our challenges and adversaries less predictable. The information that we need to sort things out has gotten, simultaneously, more diverse and more specific. Our measures of merit have also become more varied and complex, and our tool kit needs to be greatly expanded to properly address these more complex and varied situations. Dealing with this complexity will be a major challenge that requires approaching problems and tasks somewhat differently.

The term battlespace, instead of battlefield, has been used throughout this book to convey a sense of an expanded area and venue in which conflict occurs. The nature of the combatants in this battlespace is changing, and conflicts have become more public and less remote. Identifying combatants will be difficult because they will be spread out over a much wider area, either blending with their surroundings or not visible at all. Operations will be conducted in a fishbowl environment and information about events will be subject to public scrutiny in real time.

Understanding these new realities and developing appropriate strategies for dealing with them will be an ongoing challenge.

Coalition Environments

Whether in traditional military engagements, asymmetrical engagements, or in a variety of operations other than war, the United States will be working in coalition environments. Basic to the conduct of these operations is the ability to develop and maintain a shared perception of the situation, develop coherent plans that leverage the available resources, and execute them. This requires a level of information exchange, systems that can understand one another, a coalition-based planning process where all may participate, a common concept of operations, and a set of compatible procedures to carry out operations.

Given that future coalitions will be of the willing, and that they, at times, will contain former and future adversaries, achieving these prerequisites will be difficult indeed. Of greatest concern to some is that the United States, with its relatively enormous investments in technology, will become too sophisticated to interoperate with even its closest allies who cannot afford the price tags associated with the latest technologies. The need for a sufficient level of backward compatibility needs to be recognized, along with finding a way to achieve this without degrading our own performance. This is a major challenge, both technically and operationally.

Jointness

Jointness is a relatively recent concept and is now gaining momentum. In order to satisfy the needs of NCW, jointness needs to be more than skin-deep. It needs to be built-in from the bottom up, so that the best way to accomplish a mission or task, given the available information and assets, can be employed. There are significant institutional barriers to achieve *born joint* MCPs. To maximize our chances of success, we need to foster true jointness in the process of coevolution, investment strategy, and education and training efforts.

Process of Coevolution

The process of coevolution needs to differ from previous processes that served to introduce change and technology into organizations in a number of ways. First, the introduction of technology in the form of a system, or set of materials, is no longer the focus or objective. Rather, the objective is a set of NCW-based MCPs. Hence the degree of the changes required is much greater, as is the number of organizations that need to be involved. Second, adequate emphasis needs to be placed on MCPs being born joint, otherwise it is likely that stove-piped MCPs will be produced. Chances are these stove-piped MCPs will represent incremental improvements, but fail to take full advantage of the opportunities. Third, coevolution is a process of discovery and testing. The answer will not be known in advance. Thus, the process needs to be devoid of the pass/fail mentality common today. Fourth, the heart of the coevolution process is experimentation, not demonstrations nor exercises, although there is a role, albeit a reduced one, for both of these in the process. Fifth, the process is iterative. One cannot expect to get it right the first time out. However, one can expect that events will be planned and conducted to get the most knowledge out of the experience as possible.

Investment Strategy

Individual services and agencies currently acquire material and systems one by one. This approach needs to change. Instead, DoD needs to develop investment strategies and make acquisition decisions based upon portfolios. Two kinds of portfolios need to be considered. The first is a portfolio or package of investments that mirrors an MCP. The second is an infrastructure portfolio consisting of a set of capabilities necessary to support multiple MCPs in a specific area such as communications. The trade-offs that need to be made include:

1) the overall mix of MCPs to be deployed;
2) which alternate MCP configurations should be adopted for a particular mission; and
3) the components of a federation of supporting systems (including combat support, personnel, finance, etc.).

It also needs to be recognized that accounting procedures must not get in the way of making intelligent choices. Currently, expense items are not visible in the same way that capital investments are, despite the fact that the items acquired need to be part of the same portfolio. Given a budget that is unlikely to increase in real dollars and a continuing, if not increasing, tension between modernization and readiness, the systemic suboptimality inherent in current practices needs to be addressed.

Education and Training

Change is difficult. Big changes are more difficult. The adoption of NCW will involve significant, if not fundamental changes in how DoD task organizes duties and responsibilities of individuals. Individuals will need to adopt new attitudes, accept more responsibility, learn new skills, master new approaches, and operate new systems—all in a faster-paced environment. The future DoD is likely to have fewer, but more educated and highly trained individuals. Current up-and-out and job-rotation personnel practices will need to be reexamined in the face of these changes. A hard look at our whole approach to education and training is required. Given the pace of change, education and training will need to be continuous and closely integrated with day-to-day activities. Distance learning and on-the-job training, employing sophisticated tools embedded in operational systems, will become the norm. A major consideration is that we are moving away from a situation in which we knew how we wanted a particular task performed, and then designed tools and processes to teach known solutions. We are now entering a period where we will not know the answer at the start of the process, and the techniques and tools that are associated with education and training may no longer be valid.[111]

It is fitting that this book on NCW concludes with this discussion of the impact on people. The C4ISR

Cooperative Research Program has been involved in a number of lessons learned analyses of deployments and operations. An observation common to all of these was the critical contribution that individuals had upon the success of these operations. Individuals were able to overcome unfavorable initial conditions, adapt outmoded approaches and processes, and provide the work necessary to integrate technology that simply was not yet ready for prime time. If NCW is to be successful, every effort must be made to recruit, educate, and train the right people, and give them the flexibility to make the necessary adjustments.

Bringing It All Together

The Information Revolution is upon us. It is not about information technology per se. Rather it is about how information-enabled organizations are emerging as dominant forces in their respective domains. Even at this early stage in the Information Revolution we have seen how organizational forms, processes, and applications of technology have coevolved. In the commercial sector, market forces provide a continuous forcing function for coevolution. In the domain of warfare, the forcing function is discontinuous. In previous generations, warfighting concepts and capabilities have evolved slowly, if not at all during interwar periods. This is not to say that innovative ideas were not born and nurtured, during interwar periods, but rather, that with rare exceptions, they were not brought to full fruition and implemented. The crucible of war creates a new competitive dynamic. New ideas and concepts have a better opportunity to see the light of day because it often becomes clear that current operational concepts are failing.[112] Changes are accelerated and compressed into the time frame of war. Most anticipate that future conflicts will be much shorter in duration, thus not providing as good an opportunity for coevolution. Thus, without reversing this trend, we will not be able to fully realize the opportunities provided by information technologies to transform the way we do business. Our commitment to experimentation at the Joint and Service level can provide the necessary but not sufficient forcing function for the coevolution of a network-centric force. Exploiting the insights we develop through experimentation requires more. Leadership will be necessary to ensure that:

1) conditions for innovation exist at all levels;
2) promising new ideas have a chance to develop and reach maturity; and
3) legacy ideas and their manifestations do not crowd out their "competition."

This is an exciting time.

Endnotes

[1] VAdm Arthur K. Cebrowski, USN, and John J. Garstka, "Network Centric Warfare: Its Origin and Future," *Proceedings of the Naval Institute* 124:1 (January 1998): 28–35.

[2] Adm Jay L. Johnson, Chief of Naval Operations (CNO), USN, in his address at the U.S. Naval Institute Annapolis Seminar and 123rd Annual Meeting, in Annapolis, Maryland, on April 23, 1997, said the military is in the midst of "a fundamental shift from what we call platform-centric warfare to something we call network-centric warfare."

[3] U.S. Air Force, *The Army Air Forces in World War II—Vol. I: Plans and Operations, January 1939–August 1942* (Chicago: University of Chicago Press, 1948), 597–611.

[4] U.S. Air Force, *The Army Air Forces in World War II—Vol. III: Europe: Argument to VE Day, January 1944–May 1945* (Washington, DC: Office of Air Force History, 1983), 49.

[5] Richard Hough and Denis Richards, *The Battle of Britain* (New York: W. W. Norton and Company, 1989).

[6] Stephen C. Mooney, *The Cyberstate* (Denver, CO: ACM, Inc., 1996).

[7] Robert G. Phelan, Jr. and Michael L. McGinnis, "Reengineering the United States Army's Tactical Command and Control Operational Architecture for Information Operations," *Proceedings of the 1996 Winter Simulation Conference*, 1996.

[8] Richard Saul Wurman, *Information Anxiety* (New York: Bantam Books, 1990).

[9] *Ibid.*

[10] M. Mitchell Waldrop, *Complexity: The Emerging Science at the Edge of Chaos* (New York: Simon and Schuster, 1992), 259–260.

[11] Peter Newcomb, "The First Billion Takes a Lifetime...Except in the Internet Age," *Forbes* 163:8 (April 19, 1999): 246–247.

[12] T. X. Hammes, "War Isn't a Rational Business," *Proceedings of the Naval Institute* 124:7 (July 1998): 22–25.

[13] U.S. Department of Commerce, "IT Industries—Of Growing Importance to the Economy and Jobs," Appendix 1 in *The Emerging Digital Economy* (Washington, DC: Government Printing Office).

[14] Michael E. Porter, *Competitive Advantage: Creating and Sustaining Superior Performance* (New York: Free Press, 1985).

[15] Charles B. Stabel, et al., "Configuring Value for Competitive Advantage: On Chains, Shops, and Networks," *Strategic Management Journal* 19 (1998), 413–437.

[16] "George Gilder's Telecosm: Metcalfe's Law and Legacy," *Forbes ASAP* 152: Supplement (September 1993), 158–166. Metcalfe's Law is named after Robert Metcalfe, who invented the staple networking topology, Ethernet. Metcalfe's Law of the telecosm states that the potential value of a network is "n" squared, with "n" being the number of nodes on the network.

[17] *CIO Imperative: Business Results Are the End—Information Sharing Is the Means*, The Concours Group, 1997.

[18] Don Tapscott, *The Digital Economy: Promise and Peril in the Age of Networked Intelligence* (New York: McGraw-Hill, 1996), 143–152.

[19] Karl Sabbagh, *Twenty-First Century Jet: The Making and Marketing of the Boeing 777* (New York: Scribner, 1996).

[20] Carl W. Stern, "The Deconstruction of Value Chains," *Perspectives*, The Boston Consulting Group, September 1998.

[21] Karl Sabbagh, *Twenty-First Century Jet: The Making and Marketing of the Boeing 777* (New York: Scribner, 1996).

[22] *Capitalizing on Innovation*, Capital One's 1998 Debt Equity Conference, October 20, 1998.

[23] www.dell.com

[24] Joan Magretta, "The Power of Virtual Integration: An Interview with Dell Computer's Michael Dell," *Harvard Business Review* 76:2 (March–April 1998), 72–84.

[25] www.compaq.com

[26] Don Tapscott, *The Digital Economy: Promise and Peril in the Age of Networked Intelligence* (New York: McGraw-Hill, 1996), 84, 101, 131.

[27] *Ibid.*

[28] "The Leaders in 1997 Sales and Profits," *Business Week* 3567 (March 2, 1998), 110.

[29] James F. Moore, *The Death of Competition: Leadership and Strategy in the Age of Business Ecosystems* (New York: HarperBusiness, 1996), 161–188.

[30] Christopher Palmeri, "Believe in Yourself, Believe in the Merchandise," *Forbes* 160:5 (September 8, 1997), 118–124.

[31] Frank Swoboda, "Talking Management with Chairman Welch," *The Washington Post* (March 23, 1997, Section H: Business), 1, 7.

[32] John Foley, "Squeezing More Value from Data," *Information Week* (December 9, 1996), 44.

[33] Matthew Schifrin and Erika Brown, "Merrill's Malaise," *Forbes* 163:7 (April 5, 1999), 108–114.

[34] Merrill Lynch Site Visits, August 11, 1997 and October 28, 1997.

[35] Seth Schiesel, "The No. 1 Customer: Sorry It Isn't You," *The New York Times* (November 23, 1997, Section 3: Money & Business), 1, 10.

[36] Interviews with Christopher J. Carroll, Managing Director, Head of Global Electronic Trading, Deutsche Morgan Grenfell, Inc., 1996–1997.

[37] VAdm Arthur K. Cebrowski, USN, "Network Centric Warfare: An Emerging Military Response to the Information Age," Presentation to the 1999 Command and Control Research and Technology Symposium, Naval War College, Newport, RI, June 29, 1999.

[38] David S. Alberts and Richard E. Hayes, *Command Arrangements for Peace Operations* (Washington, DC: National Defense University Press, 1995); David S. Alberts, *Operations Other Than War: The Technological Dimension* (Washington, DC: National Defense University Press, 1995); Margaret Daly Hayes and Gary F. Wheatley, *Interagency and Political-Military Dimensions of Peace Operations: Haiti—A Case Study* (Washington, DC: National Defense University Press, 1996); Tom Czerwinski, *Coping with the Bounds: Speculations on Nonlinearity in Military Affairs* (Washington, DC: National Defense University Press, 1998); Larry Wentz, *Lessons from Bosnia: The IFOR Experience* (Washington, DC: National Defense University Press, 1998); Martin C. Libicki, *What Is Information Warfare?* (Washington, DC, National Defense University Press, 1995); and Martha Maurer, *Coalition Command and Control: Key Considerations* (Washington, DC: National Defense University Press, 1994).

[39] David S. Alberts, *Command and Control in Peace Operations*, [report on "Western Hemisphere Experience in

Global Peace Operations," the third of a series of reports of workshops organized by the INSS Center for Advanced Command Concepts and Technology (ACTS)] (Washington, DC: National Defense University Press, 1995).

[40] *Ibid.*

[41] Martin C. Libicki, *What Is Information Warfare?* (Washington, DC: National Defense University Press, 1995).

[42] Stuart E. Johnson and Martin C. Libicki, "DBK and Its Consequences," in *Dominant Battlespace Knowledge* (Washington, DC: National Defense University Press, 1995), 34.

[43] Kenneth Allard, *Somalia Operations: Lessons Learned* (Washington, DC: National Defense University Press, 1995).

[44] Joseph A. Welch, Jr., "State of the Art of C2 Assessment," *Proceedings for Quantitative Assessment of the Utility of Command and Control System*, MTR 80W00025 (January 1980), 11.

[45] For details on Lawson's model, see "Naval Tactical C3 Architecture, 1985–1995," *Signal* 33:10 (August 1979), 71–72.

[46] For details, contact Evidence Based Research, Inc., at www.ebrinc.com

[47] Kenneth Allard, *Command, Control, and the Common Defense*, revised edition (Washington, DC: National Defense University Press, 1996).

[48] Interviews with RAdm Charles R. McGrail, USN (Ret.), 1996-1998.

[49] Larry Wentz, *Lessons from Bosnia: The IFOR Experience* (Washington, DC: National Defense University Press, 1998).

[50] Pascale Combelles Siegel, *Target Bosnia: Integrating Information Activities in Peace Operations* (Washington, DC: National Defense University Press, 1998).

[51] Manuel de Landa, *War in the Age of Intelligent Machines* (New York: Zone Books, 1991); John T. Dockerty and A. E. R. Woodcock, *The Military Landscape: Mathematical Models of Combat* (Cambridge, UK: Woodhead, 1993); Murray Gell-Mann, *The Quark and the Jaguar* (New York, W.H. Freeman, 1994); John Gore, *Chaos, Complexity, and the Military* (Washington, DC: National Defense University, 1996); Glenn E. James, *Chaos Theory: The Essentials for Military Applications* Newport Paper 10 (Newport, RI: Naval War College, 1996); and Edward N. Lorenz, *The Essence of Chaos* (Seattle, WA: University of Washington Press, 1993). For more, see David S. Alberts and Thomas J. Czerwinski, "Working Bibliography," *Complexity, Global Politics, and National Security* (Washington, DC: National Defense University Press, 1997), 333–381.

[52] David S. Alberts, *Lessons Learned from ISX 1.1*, AIAA Joint Experiment Task Force Briefing, January 28, 1999.

[53] *Knowledge and Speed: The Annual Report on the Army After Next Project to the Chief of Staff of the Army*, July 1997.

[54] *Executive Summary of Global '98 Wargame*, Naval War College, Newport, RI, July 13–31, 1998.

[55] *Ibid.*

[56] *Ibid.*

[57] *Ibid.*

[58] David A. Fulghum, "Improved Air Defenses Prompt Pentagon Fears," *Aviation Week & Space Technology* 149:1 (July 6, 1998), 22–24.

[59] VAdm Arthur K. Cebrowski, USN, and John J. Garstka, "Network Centric Warfare: Its Origin and Future," *Proceedings of the Naval Institute* 124:1 (January, 1998), 28–35.

[60] Adm Jay L. Johnson, CNO, USN, Address at the U.S. Naval Institute Annapolis Seminar and 123rd Annual Meeting, Annapolis, MD, April 23, 1997.

[61] David S. Alberts, *The Unintended Consequences of Information Age Technologies* (Washington, DC: National Defense University Press, 1996), 35–36.

[62] *Executive Summary of Global '98 Wargame*, Naval War College, Newport, RI, July 13–31, 1998.

[63] *Ibid.*

[64] Gen. Charles A. Horner, USAF (Ret.), "Comments on Expeditionary Force Experiment '98," *C2 Earlybird: Special Edition EFX '98 Lessons Learned* 1: Special Ed.1 (December 1998).

[65] Robert M. Nutwell, "IT-21 Provides Big 'Reachbacks'," *Proceedings of the Naval Institute* 124:1 (January 1998), 36–38.

[66] Adm Jay L. Johnson, CNO, USN, CNO Address at AFCEA West, San Diego, CA, January 21, 1998.

[67] R. Thomas Goodden, et al., *Education Technology in Support of Joint Professional Military Education in 2010: The EdTech Report* (Washington, DC: A Joint Staff Publication, October 1998).

[68] *Tactics, Techniques, and Procedures for the Common Operational Modeling, Planning, and Simulation Strategy (COMPASS), Version 1.1*, JWID Joint Project Office, August 31, 1998.

[69] In addition to sensor, decision maker, and actor entities that work together to achieve and utilize battlespace awareness, there are supporting entities that structure the flow of material and systems that process battlespace information.

[70] A common operational picture does not imply that everyone in the battlespace sees exactly the same thing, in the same way, at the same time. Rather it means that at least a subset of the people have the same information available about key components of battlespace awareness in a timely manner. The effect is that they share a common perception of the situation. This common perception enables better communication and mutually supporting actions.

[71] Sarah Cliffe, "Knowledge Management: The Well-Connected Business," *Harvard Business Review* 76:4 (July–August 1998), 17–21.

[72] Air Force Space Command/Space Warfare Center, *Information Briefing on Capabilities of Space Warfare Center/ Shield Program*, Colorado Springs, CO, 1998.

[73] *Sensor-to-Shooter C4 Battle Management, Final Report* (Washington, DC: C4ISR Decision Support Center and Joint Chiefs of Staff Directorate for C4 Systems, April 1, 1999).

[74] William K. Stevens, "Naval Simulation System: Representation of Network Centric Warfare Concepts and Architectures," *Proceedings of the SMi Conference on Network Centric Warfare*, June 23-24, 1999, London.

[75] Andy McNab, *Bravo Two Zero*, New York, Island Books, 1994, 25-28.

[76] See U.S. Marine Corps, *Beyond C2: A Concept for Comprehensive Command and Coordination of the Marine Air-Ground Task Force* (Washington, DC: Headquarters, U.S. Marine Corps, June 1998).

[77] David S. Alberts and Thomas J. Czerwinski, "Working Bibliography," *Complexity, Global Politics, and National* Security (Washington, DC: National Defense University Press, 1997), 333–381; and Tom Czerwinski, *Coping with the Bounds: Speculations on Nonlinearity in Military Affairs* (Washington, DC: National Defense University Press, 1998). Also, visit the Santa Fe Institute Internet homepage at www.santafe.edu

[78] The word "system" here should not be taken to mean computer systems, but refers to a collection of interacting individuals and organizations, along with their processes and tools.

[79] VAdm Arthur K. Cebrowski, USN, and John J. Garstka, "Network Centric Warfare: Its Origin and Future," *Proceedings of the Naval Institute* 124:1 (January 1998), 28–35.

[80] *Knowledge and Speed: The Annual Report on the Army After Next Project to the Chief of Staff of the Army*, July 1997.

[81] John A. Tirpak, "Deliberate Force," *Air Force* 80:10 (October 1987).

[82] Tempo here refers to the pace of the engagement, how fast decisions are made and acted upon, and how many simultaneous decision/action threads can be concurrent. Operating tempo is a different term that has been used to describe the utilization of equipment. A high operating tempo means that the useful life (in calendar time) of a piece of equipment will reduce and/or increase maintenance costs.

[83] Maneuver also includes being put in the right place the first time.

[84] "The Cooperative Engagement Capability," *Johns Hopkins APL Technical Digest* 16:4 (1995), 377–396.

[85] *Sensor to Shooter III: Precision Engagement C4ISR Architecture Analysis, Final Report* (Washington, DC: C4ISR

Decision Support Center and Joint Chiefs of Staff Directorate for C4 Systems, June 15, 1997).

[86] VAdm Arthur K. Cebrowski, USN, and John J. Garstka, "Network Centric Warfare: Its Origin and Future," *Proceedings of the Naval Institute* 124:1 (January 1998), 28–35.

[87] Interview of MG William S. Wallace, CG 4th ID, USA, Fort Hood, TX, January 20, 1999.

[88] VAdm Arthur K. Cebrowski, USN, Written testimony to hearing on Defense Information Superiority and Information Assurance—Entering the 21st Century, held by House Armed Services Committee, subcommittee on military research and development and subcommittee on military procurement, February 23, 1999.

[89] BG William L. Bond, USA, *Army Digitization Overview*, Briefing to Dr. Jacques Gansler, USD (A&T), at the Pentagon, Arlington, VA, on May 20, 1998.

[90] BG William L. Bond, USA, *Military CIS '98*, Briefing to Dr. Jacques Gansler, USD (A&T), at the Pentagon, Arlington, VA, on April 20, 1998.

[91] http://efx.acc.af.mil, updated 01/21/99.

[92] *Smart Card in Cobra Gold '98: Business Case Analysis—Final Report*, Department of Defense Smart Card Technology Office, January 1999. [Report available at www.dmdc.osd.mil/smartcard].

[93] Harlan Ullman, James Wade, Jr. et al., *Shock and Awe: Achieving Rapid Dominance* (Washington, DC: National Defense University Press, 1996).

[94] Artificial because the limits are the result of how we choose to distribute responsibility and utilize information rather than the results of information availability and quality.

[95] Sherry Sontag and Christopher Drew, *Blind Man's Bluff: The Untold Story of American Submarine Espionage*, Public Affairs™, 1998.

[96] LTG Douglas D. Buchholz, USA, Written testimony to hearing on defense transformation, held by Senate Armed Services Committee, subcommittee on airland forces, March 4, 1998.

[97] VAdm Arthur K. Cebrowski, USN, and John J. Garstka, "Network Centric Warfare: Its Origin and Future," *Proceedings of the Naval Institute* 124:1 (January 1998), 28–35.

[98] Michael S. Frankel and Robert H. Gormley, "Achieving Information Dominance: The Integrated Information Infrastructure—A Vision for the 21st Century," *SRI International Study Report*, September 17, 1998.

[99] *CISCO Internetwork Operating System—Release 12.0*, CISCO Systems, Copyright 1989–1998.

[100] Website for Report of President's Commission on Critical Infrastructure Protection, [www.rstcorp.com/ieee/archives], March 1999.

[101] Lt.Gen. John L. Woodward, USAF, Written testimony to hearing on Defense Information Superiority and Information Assurance—Entering the 21st Century, held by House Armed Services Committee, subcommittee on military research and development and subcommittee on military procurement, February 23, 1999.

[102] That is, they no longer result from a directed search for an improved capability to fill a perceived existing or projected operational shortfall (e.g., more accurate, longer range weapons, stealth technology, improved armor).

[103] AFCEA Study Team, *Evolutionary Acquisition Study* (Fairfax, VA: AFCEA, June 7, 1993).

[104] *Ibid.*

[105]David S. Alberts, *Lessons Learned from ISX 1.1*, AIAA Joint Experiment Task Force Briefing, January 28, 1999.

[106]These ideas were developed by an AIAA Task Force on C2 Experimentation.

[107] *Sensor to Shooter III: Precision Engagement C4ISR Architecture Analysis, Final Report* (Washington, DC: C4ISR Decision Support Center and Joint Chiefs of Staff Directorate for C4 Systems, June 15, 1997).

[108]Joseph A. Welch, Jr., "State of the Art of C2 Assessment," *Proceedings for Quantitative Assessment of the Utility of Command and Control System*, MTR 80W00025 (January 1980), 11.

[109]Adm Archie R. Clemins, USN, "Naval Simulation System (NSS): An Assessment of IT-21 Warfighting Value-Added," Briefing, January 5, 1999.

[110]*Measuring the Effects of Network-Centric Warfare* (Draft, Unpublished), Office of the Secretary of Defense (Net Assessment), Pentagon, Arlington, VA.

[111]Obviously, at any given point in time, we need to settle in on the tasks to be accomplished, associated doctrine, and a set of systems. However, a significant amount of effort needs to be devoted to developing new approaches and systems if we are to adopt NCW and that we will, in future, evolve these far more rapidly than we evolve current practices and systems. Therefore, our approach to education and training needs to be adapted to the task of developing NCW MCPs and evolving them.

[112]U.S. Air Force, *The Army Air Forces in World War II—Vol I: Plans and Operations, January 1939–August 1942* (Chicago: University of Chicago Press, 1948), 666–668.