The Unintended Consequences of Information Age Technologies

Written By

DR. DAVID S. ALBERTS

DIRECTOR, DIRECTORATE OF ADVANCED CONCEPTS, TECHNOLOGIES,
AND INFORMATION STRATEGIES (ACTIS)

NATIONAL DEFENSE UNIVERSITY

NDU Press Book

April 1996

Table of Contents

Introduction

Military organizations are, by their very nature, resistant to change. This is, in no small part, due to the fact that the cost of error is exceedingly high. Change, particularly change that may affect the relationships among organizations and between commanders and their subordinates, presents significant risks and generates considerable concern.

The explosion of information technologies has set in motion a virtual tidal wave of change that is in the process of profoundly affecting organizations and individuals in multiple dimensions. The military is no exception. At the very beginning of the information age, technological advances made it possible to provide more complete, more accurate, and more timely information to decision makers. As the costs of processing and communications power tumbled, it became cost-effective for organizations to adopt and utilize information technologies in more and more situations.

Military organizations have traditionally provided information to forces in three ways: commands, intelligence, and doctrine. Commands serve to define the specific task at hand. Intelligence provides information about the environment in which the task is to be carried out. Doctrine provides the "rules of the game" or standard operating procedures. Doctrine, unlike commands and intelligence, is not provided in real time, but serves to shape the culture and mind sets of the individuals involved. Thus, information has, until recently, been inseparable from commanders, command structures, and command systems. Each of these three ways of communicating information about what is expected of subordinate organizations and individuals has evolved over time to be mutually supportive of an overall command concept or approach matched to the nature of the conflict and the capabilities of the forces. The success of military operations depends to a large extent upon the ability to coordinate activities to achieve synchronized operations. Ensuring that individuals behave as intended or as expected in the face of uncertainty ("the fog of war") and under stress is a key to achieving coordinated activities. The selective dissemination of information has been used as a tool to define and shape the environment in which soldiers operate to ensure conforming behavior.

The military is now on the road to becoming an information age organization. The transformation involved is fraught with both risks and opportunities because it will affect the nature of the information provided as well as the manner in which it is provided.

Background and Purpose

The C4I for the Warrior (C4IFTW) concept that currently guides the military's adoption of information technologies involves the provision of vastly increased access to information at all echelons. The full implications and consequences of achieving the stated goals and objectives of C4IFTW will, of course, not be clear for years to come. The analysis reported upon herein was initiated as a result of concerns expressed by the Chairman of the Joint Chiefs of Staff regarding the unintended consequences of providing too much access to information.

Implicit in the concerns being expressed by the Chairman and others throughout the Department of Defense (DoD) are uncertainties about the impact of separating information flows from the command structure and the effects of almost unlimited amounts of information upon decision making. Questions remain regarding exactly how much information should be provided to each echelon. For example, how does the provision of information relate to a unit's mobility and lethality? The appropriate command concepts for an information-rich battlefield have, as yet, not been determined even at the most basic level. Concerns have been raised regarding the potential adverse effects of increased visibility into operations at all levels, including potential for information overload, second guessing, micro-management, stifling of initiatives, and distraction.

A separate but related set of concerns involves the manner in which our potential adversaries adopt and utilize these technologies and the capabilities that result. A final set of concerns involves our ability to protect information and information assets and to deal with failures of and degradations in the systems that provide information to decision makers, shooters, and others with crucial roles.

The purpose of this analysis is to identify a strategy for introducing and using information age technologies that accomplishes two things: first, the identification and avoidance of adverse unintended consequences associated with the introduction and utilization of information technologies; and second, the ability to recognize and capitalize on unexpected opportunities.

Given that our potential adversaries have access to virtually the same information technologies that we have, the margin for victory will be the degree to which we manage our trans-formation into the information age. Our ability to integrate a wide variety of systems into a true system of systems will depend not only upon our technical skills but also upon how well we adapt our doctrine, organizations, and culture to take advantage of the opportunities that technology affords.

Observations

In the search for a solution to the problem of adverse unintended consequences inherent in the adoption of information technologies, care must be taken to define an approach that is enabling rather than limiting. Some argue that the problems and risks associated with change can be addressed simply by avoiding significant changes. Others advocate that changes be introduced slowly and systematically, thoroughly testing proposed alterations until the probability of error is acceptably low. In many circum-stances, these very conservative approaches may be appropriate. In this case, they are not.

We are not in a position to take the apparently safe and comfortable road to the introduction of change. The environment in which we must operate is being transformed in a number of critical dimensions; consequently, business as usual (the default decision) carries with it significant adverse consequences of its own. Thus, "doing nothing" is neither conservative nor safe.

The low cost of obtaining information age technologies will help potential adversaries improve their military capabilities as they learn to leverage these technologies effectively. Thus, inaction will lead down a path that exposes us to new and improved adversary capabilities that we may not be able to counter effectively without change. In addition, in an era in which budgetary pressures will continue, a failure to take advantage of opportunities to improve cost effectiveness translates into less capability.

The pace of the advances in information technologies and their adoption make it imperative that our approach to change must be capable of keeping pace or it is doomed to failure from the start. Further, we must recognize that there are two kinds of risks associated with the selection of an approach to change. In addition to the widely recognized risks associated with adverse consequences, there are the risks associated with failure to recognize and capitalize on unexpected opportunities to do things more effectively and efficiently. Thus, risk management becomes the name of the game.

Since we cannot stop, slow down, or control the information explosion or totally prevent unintended consequences, we must design a strategy for introducing information technologies that a) identifies and anticipates negative repercussions and enables us to avoid those repercussions or minimize their impacts, b) recognizes and takes advantage of unexpected opportunities, and c) balances the risks associated with the failure to achieve these two objectives. This strategy must also be capable of facilitating change fast enough to keep pace with exogenous forces impacting technologies and technologies' adoption by potential adversaries.

A technology insertion strategy designed to fully leverage information technologies requires alterations in our concepts of operation, doctrine, organizations, and force structure. Associated changes in logistics, education, and training will also be required. Without these changes, we will only obtain incremental improvements in effectiveness and efficiency while foreclosing opportunities for the order of magnitude improvements necessary to maintain the winning edge.

Executive Summary

After analyzing the pros and cons of following the path specified by C4IFTW, it is clear that the potential benefits of information technology far outweigh the potential costs associated with unintended consequences. The specific concerns raised regarding the deleterious effects of excessive information access can be addressed.

However, a cautionary note needs to be struck. The above conclusion is predicated upon the adoption of an effective technology insertion strategy. Without the adoption of a comprehensive and systematic process for introducing and using these technologies, their positive potential will not be realized and the probability of adverse impacts will increase to unacceptable levels.

Business as usual is truly a prescription for disaster. It is recommended that leadership at all levels clearly articulate the need to move out smartly on the transformation to an information age military, a military that embraces rather than resists the changes permitting the full leverage of opportunities afforded by information age technologies. It is further recommended that appropriate investment strategies be developed and supported at the highest levels.

The technological insertion approach proposed here, based upon mission capability packages, stresses that all types of changes required to fully exploit emerging technologies and to manage the consequent risks must be developed as a coherent group. Any new mission capability package also needs to be tested and refined before widespread adoption will be appropriate. Therefore, it is recommended that a joint mission be selected to serve as a prototype to examine the nature of the changes necessitated by the information age and to test the mission capability package approach for developing concepts and implementing change.

Success requires innovative ideas. It is recommended that leaders across the board encourage the development and strengthening of centers of innovation within their organizations.

Information Technology Impacts on the Warfighter

Impacts on the Warfighter

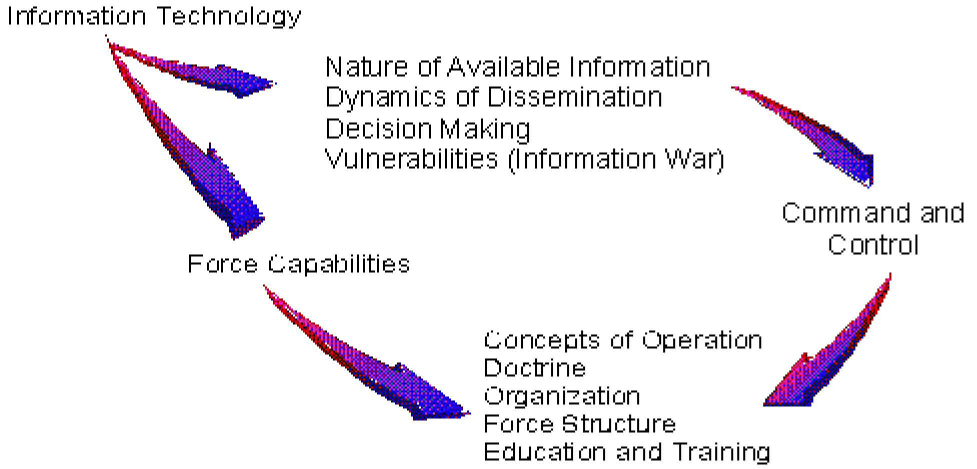
Information technologies, for the purposes of this analysis, include collection, processing, display, and communications technologies. Processing technologies include data fusion and analysis as well as support for decision making, such as knowledge-based expert systems.

Advances in these technologies have resulted in an enormous amount of near real-time information being potentially available to individuals anywhere at anytime. The "intelligence" level of systems and our confidence in their ability has also increased dramatically to the point where life and death decisions are now routinely being made automatically by computers, albeit with some degree of human supervision.

Even at this early point in the information age, the battlefield is awash with vastly increased amounts and improved quality of information. The dynamics of information dissemination have changed considerably in the latter half of this century, from flowing primarily through command structures to the point where significant amounts of information are obtained outside of the command hierarchy. Thus, what was once a predominantly highly constrained and vertical information flow has evolved into a mix of vertical and horizontal flows. Naturally, the amount, quality, and dynamics of information dissemination have begun to impact the ways decisions are allocated (delegation) and the manner in which those decisions are made.

Thus (as shown in Figure 1), advances in information technologies provide us with significant opportunities both to improve our ability to command and control our forces and to add to and/or improve our force capabilities.

Figure 1. IT Impacts on the Warfighter



Our information-related vulnerabilities have also increased. Increased reliance on high-tech systems for information collection, interpretation, processing, analysis, communication, and display has made failures in these systems more disruptive. The ubiquitous nature of these technologies provides our potential adversaries with capabilities that help them understand how to attack our information assets and give them the tools to do so. Our command and control systems can no longer be evaluated on the basis of measures of merit (MOMs) related solely to the production of quality information in a timely manner. It is now important to consider such attributes as availability, integrity, and authenticity of the information, its ease of use, and its value-added for decision making.

Command and control has long been a recognized force multiplier, and improvements in information technologies offer tremendous opportunities to perfect existing approaches and explore new ones. Quicker, better decisions will allow us to operate more effectively within the enemy's decision cycle, providing us with an opportunity to control engagements. Improvements in information technologies also enhance the capabilities of our weapons, providing them with increased standoff capability and accuracy.

But the opportunities that new and improved weapons and command and control offer cannot be successfully exploited unless we make appropriate changes to our concepts of operations, doctrine, and organizational structures and provide the required personnel education, training, and programs of exercises.

This is not to imply that we must wait for improvements in technology to actually occur before considering new approaches to command and control, concepts of operation, doctrine, or organizational arrangements. Quite the contrary, if we wait, the inertia associated with developing and implementing these changes will permanently keep us behind the technological power curve. Nor does this imply that changes in command and control or force capabilities must necessarily precede alterations to concepts of operation or doctrine.

In reality, these elements (e.g. concept of operations, doctrine, technology, etc.) constitute a package that, taken as a whole, provides real operational capability that can be applied in a specific mission. A mission-specific perspective is important because no organizational structure or approach to command and control is going to be well suited for the range of likely missions, missions as diverse as an MRC and peace-keeping. New MOMs will be required which must also be mission-related. For example, classic measures, such as taking and holding territory, are not relevant in some mission contexts.

Nature of Future War

Future war can be envisioned as consisting of three general classes of activities. First, there is the perfection of traditional combat. Second, there is the evolution of what have been called non-traditional missions, a very mixed bag of activities including humanitarian assistance, SOLIC operations, counter-drug operations, peace operations, and counter-proliferation. Third, there is the birth of a form of war unique to the information age.

Information technology not only will change the nature of what we know today as war and operations other than war, but also will spawn a new set of activities that will become familiar to future generations as constituting "warfare" in the 21st century. Today, we might have some difficulty in viewing this set of activities as "war" or as the concern or responsibility of DoD. Current planning and budgeting approaches find it difficult to address these aspects of the future, since they are not extensions of existing military missions and responsibilities.

However, in each of these three cases, information technologies will shape the battlespace and define the possibilities.

Future "Traditional" Combat

The future conventional battlespace will be neither contiguous nor orderly. Tempo will be extraordinarily high by today's standards. Given expected improvements in weapons and command and control, if a target can be seen it will be destroyed. Therefore, survival will depend upon organic defensive capability, suppression, and stealth.

Concepts of operation will center around massing fires rather than forces. Command and control concepts will involve dynamic tradeoffs between ensuring that Rules of Engagement (ROEs) are followed, prioritizing targets, and minimizing the time required to pass information from sensor to shooter.

Commanders will have more direct influence on shaping the battlespace and influencing the initial conditions of the engagement. Staffs will be significantly reduced as organizational structures flatten. Most commands will be automatically disseminated and incorporated in decision aids. Many decisions will be fully automated. Virtually all information will be distributed horizontally.

In short, many significant changes will need to be made to respond to the challenges of the information age. With this much change foreseen down the road, care must be exercised to ensure success.

Evolution of Non-Traditional Missions

Since the end of the Cold War, the nation has looked to DoD not only to reduce overall spending, but also to undertake a more diverse set of roles, both at home and around the globe. The unique capabilities developed by the U.S. military to meet the global challenge posed by the Soviet Union and maintained to protect U.S. interests around the world are seen as national assets that can be employed beyond their traditional combat and combat service support roles. Global air and sea lift are important for disaster relief, crisis intervention, humanitarian assistance, and support to peace operations. Similarly, the secure global communications capacity of the U.S. military is a crucial asset in a wide range of situations. The capability of the military to surge from its training bases and to react rapidly when dangerous situations arise far exceeds the capacities of most civilian agencies, for whom surge capacity is a slow and cumbersome process and crisis response is an alien practice. These unique capabilities, combined with the absence of an urgent, direct military threat, have caused the nation to expect greater involvement by DoD in non-traditional missions, such as humanitarian assistance, maintaining law and order when local and state authorities cannot, disaster relief, and countering drug smuggling and the proliferation of weapons of mass destruction.

The international environment has also changed in ways that make non-traditional missions more likely and more diverse. The absence of a single military threat and the need for international legitimacy when force is threatened or used have made coalition operations the norm rather than the exception. International organizations, particularly the United Nations, have become increasingly assertive and have pressed a vision of global interests in peace and cooperation. As the only remaining global superpower, the United States is expected to respond whenever international peace and harmony are threatened and the nations of the world feel action is needed. This has been interpreted to mean that the U.S. must lead when the peace is threatened, international crimes are committed, or human tragedy looms.

The growing internationalism is undercut by parochial clashes and conflicts. Freed from the smothering constraints of communist governments, national movements in Eastern Europe and the former USSR have proven willing to challenge the peace to seek independence. Clans and tribes in Africa have reasserted their interests, sometimes violently. Asia is the site of arms races and uncertain relations between nations. Domestic and international struggles for the long-term control of the Middle East oil wealth and the worldwide resurgence of fundamentalist Islam add to the dangerous international situation. Drug traffickers present a frustrating cross-border challenge. Recent attention has also focused on conflicts arising from environmental issues, particularly disputes over water rights, ocean areas, and transboundary air pollution.

Perhaps most important, media coverage and recent successes have led to very high expectations about the performance of the U.S. military. Minimum casualties among both com-bat forces and civilians is widely perceived as an important and achievable goal. At the same time, the military is expected to be effective by accomplishing missions precisely and quickly. Finally, all this is expected within the context of declining budgets.

Warfare in the Information Arena

As the global society enters the information age, military operations inevitably have been impacted and transformed. Satellite communications, video conferencing, battlefield facsimile machines, digital communications systems, personal computers, the Global

Positioning System, and dozens of other transforming tools are already commonplace. Moreover, DoD has gone from being the driving force in information technology to being a specialty user with a new reliance on commercial-off-the-shelf (COTS) technology in order to acquire and field cost-effective systems. The widespread proliferation of this technology, as well as the increased reliance on COTS, has contributed to a significant increase in our vulnerablity.

The implications of warfare in the information arena are enormous. First, national homelands are not sanctuaries. They can be attacked directly, and potentially anonymously, by foreign powers, criminal organizations, or non-national actors such as ethnic groups, renegade corporations, or zealots of almost any persuasion. Traditional military weapons cannot be inter-posed between the information warfare threat and society.

Second, even where traditional combat conditions exist (hostile military forces face one another in a terrain-defined battlespace), kinetic weapons are only part of the arsenal available to the adversaries. Indeed, electronic espionage and sabotage, psychological warfare attacks delivered via mass media, digital deception, and hacker attacks on the adversaries' command and control systems will be used to neutralize most traditional forces and allow concentration of fire and decisive force at the crucial time and place in the battlespace.

However, warfare in this information age will require enormously complex planning and coordination, very near real time and total situation awareness, decision support systems that filter and fuse information very rapidly and perform simple plan extensions and revisions almost automatically, and massive database and information exchange capabilities to track both friendly and enemy situations as well as rehearse and forecast battlespace dynamics.

This rapidly evolving situation means that the U.S. military must be able to perform the following three fundamental information warfare missions: 1) protect its own information systems, 2) attack and influence the information systems of its adversaries, and 3) leverage U.S. information to gain decisive advantage in a battlespace where national security is threatened.

Concerns and Remedies

C4IFTW will bring about a series of changes that will profoundly affect both the nature of information available to the warfighter and how this information will be disseminated. Concerns arise regarding the impacts that these changes will have on the decision process and upon decision makers. Other concerns involve new or increased vulnerabilities associated with information age systems and processes. Finally, a set of concerns centers on our ability to design and acquire systems given the information age realities of increased reliance on COTS hard-ware and software and the ever-shrinking technology life cycle.

An analysis of the specific concerns identified revealed that suggested remedies fell into the following groups:

- Concepts/Doctrine
- Education Training, and Exercise
- Testing System Design and Specifications
- Organization and Procedures
- Tools, Models, and Decision Aids

Specific issues, grouped into the five areas identified above, were identified and examined against the types of remedies appropriate to avoid or manage them. As these areas were reviewed and remedies considered, the same basic set of remedies arose over and over again, making it clear that a coherent program of remedies can and should be developed. The remainder of the chapter is devoted to a discussion of each of the following areas of concern and the remedies that are associated with them:

- Nature of the available information
- Dynamics of information dissemination
- Impact on military decision making
- Vulnerabilities arising from the information systems themselves
- C2 design and acquisition issues

Available Information

Non-essential information swamping critical information becomes a major issue for C4IFTW. The sheer volume of information received could frustrate the ability to quickly identify critical information for the decision at hand. To avoid situations in which more information than can be processed is presented, decisions must be made about what information is really needed, what is nice to have, what is irrelevant, and what is potentially distracting or confusing.

The requirement for information clearly depends upon both the mission and the situation. Unless individuals are given an opportunity to think through what they really need, requirements for information will always be inflated. Furthermore, this cannot be a "paper" exercise. Individuals with appropriate military experience must be placed in realistic situations and must be allowed to experiment with different amounts and types of information. The lessons learned from these experiments can be used as inputs to requirements and design analyses.

While refining information-related requirements in a more systematic manner will certainly help, it will not be sufficient to avoid the effects of information overload. Better education and training, devoted to information processing under stress and in environments characterized by uncertainty, are needed to develop the necessary skills to handle these information-rich situations. System designs must track these "information domains."

Finally, practice is key to perfecting and maintaining the skills necessary to function in an information-intensive environment. Therefore, exercises, "on the job" training, and continuing professional education need to be added to complete the necessary set of "remedies" associated with increases in the amounts of information that will be provided.

Sophisticated presentations can also obscure vital information and/or mask poor quality or incomplete data. Designing presentations that illuminate issues and facilitate decision making involves tradeoffs and choices between "raw" or unprocessed data and information that contains a mixture of "fact" and inference. Often fusion algorithms or decision aids "fill in the blanks" and provide users with inferences from available data. In some cases, valuable information is lost in the process. The remedies to address this concern include those discussed above as well as the development of better visualization techniques enabling individuals to better understand the nature of the underlying data for a given presentation.

Uncertainty regarding the quality of the information being presented or its integrity could lead to a lack of confidence that inhibits use of information or intelligence systems. Decision makers clearly need confidence in the reliability, currency and accuracy of data in order to act on it. In the information age, the integrity and authenticity of the data are important as well and should be considered as additional MOMs for information. In addition to the remedies discussed above, effective defensive IW protection measures and decision aids need to be developed that can permit decision makers to rely on the authenticity and integrity of the data. Presentation techniques that convey the quality of the underlying data are an important issue in their own right.

Dynamics of Dissemination

Not only is the amount of information available dramatically increasing as the information age unfolds, our ability to widely disseminate this information is keeping pace. As information sources proliferate, individuals are increasingly receiving inputs from multiple sources in a less than coordinated manner. This asynchronous arrival of information has been found to confuse and distract decision makers. Studies have also shown that the weight individuals place upon information may be related to the order in which that information is received. This is potentially dangerous because it can lead to differences in individuals' perceptions of a situation.

The C4IFTW concept virtually assures that individuals will be receiving different information in different sequences. To avoid the potential pitfalls associated with this phenomena, education and training are needed to heighten awareness of these issues and help individuals assimilate new data into their "information domains." Doctrine is needed to ensure that behavior is consistent across the organization. Display techniques are required to facilitate information collection and analysis. Decision aids are needed to help synthesize and fuse information on a continuing basis.

As with other concerns discussed previously, practice is a key element in ensuring that individuals develop and maintain proficiencies in dealing with this potentially confusing phenomenon.

Given the thrust of defense initiatives, particularly DISA's Global Grid and the Army's efforts to digitize the battlefield, there will be an enormous increase in the amount of information moving through communication pipes. With the C4IFTW vision of a mix of information "push" and "pull" with an emphasis on "pull," inability to anticipate or control requests for information could result in system degradation, particularly in times of great stress. In these situations, vital as well as non-vital information flow may be affected. To avoid this potentially crippling scenario, appropriate policy, doctrine, and procedures regarding the use of information retrieval mechanisms need to be developed and instituted. Again, education, training, and practice are required to raise awareness of the problem and to develop the skills needed to operate in a "degraded" information environment. Network tools are also needed to provide warnings when the limits of the distribution system are being approached and to help bring the situation under control. Finally, the design of our information distribution infrastructure needs to maximize robustness. The only certainty is that systems will not be used exactly as intended or under precisely the conditions assumed in their design, development, and testing.

Decision Making

The linkages between information quality, distribution, communications patterns, and decision making are complex and diverse. A review of organization theory, group dynamics, information theory, and past research on command and control offers key insights into these linkages and how they function.

First, when information is freely available, role overlap tends to be commonplace. Superiors tend to micromanage, particularly when the stakes are high; there are no higher stakes than combat. Subordinates, however, when provided with the larger picture historically available only to senior commanders, are also likely to second guess decisions made at higher levels and (in richly connected systems) have the information required to undertake initiatives their superiors may find inappropriate. Avoiding this set of counterproductive behaviors and management practices requires doctrine, appropriate organizational structures, self-discipline, and training.

Second, decision making in an information rich environment increasingly means media attention. The pressures of a "fish bowl" environment affect performance in a variety of often adverse ways. Tendencies to overreact, to act quickly, to appear decisive despite limited information, or to "posture" for the media can only be overcome through realistic training and experience.

When decision making becomes a collective process, which tends to occur when several principals have easy access to one another in a situation they all consider important, decisions tend to converge on options that meet group consensus. This "collective wisdom" has been demonstrated in both theoretical and empirical analyses to tend strongly toward risk averse options or poorly thought out "group-think" alternatives. The "brilliant" alternative or innovative approach foreseen by one individual is unlikely to survive this deliberative process. The potential strength of this collective process, which has excelled at solving complex problems such as those at operational and strategic combat levels, can only be achieved by an open approach to command and control decision making and a doctrine that stresses individual innovation and leadership at all levels.

Fully-connected systems also reduce the need for detailed action coordination by commanders because they make available information that would have to be requested from other elements in a classic military information structure. For example, rather than having to request information about the availability of transportation assets or ammunition needed for a combat operation, a line commander will be able to check stock levels directly through the information grid. This can lead to insufficient or ineffective coordination because subject matter experts are not consulted or because more than one command makes plans to use the same asset but none has a clear commitment of asset availability. Industry experience with richly connected systems has shown that collaborative planning and decision aids (which automatically perform coordination tasks and/or pass information between nodes in decision-making structures) are needed to avoid these problems. In addition, "red team" procedures to cross-check decisions can help to ensure adequate, timely coordination.

As generations of military commanders who have become accustomed to the availability of high density and high quality data about the battlefield mature and move into senior command positions, the expectation of near perfect information and the willingness to delay decisions in the expectation of better information will grow. However, the very rapid pace of future battles, as well as the imperatives of turning inside adversary decision loops, will punish procrastination and inaction severely. The commander who waits for near perfect information will be defeated by one who acts on "good enough" information. Doctrine and effective training for commanders must instill the judgement required to differentiate between sufficient and necessary or desirable information.

Because of the increased pace of battle and the high lethality expected in future battlespace, more and more decisions will be assigned to expert systems. This will include not only "sensor to shooter" linkages where the identification, assignment, and killing of targets must be so rapid that unaided human decision making cannot keep pace; but also other complex domains characterized by rapid developments in logistics planning, air tasking order development, and medivac helicopter routing. However, development, testing, and training are inadequate to ensure confidence in these systems. Testing is particularly important. Technology demonstrations are a good, cost effective way to gain user feedback and to develop positive attitudes toward these systems, but operational testing in realistic field conditions is also necessary to avoid systems failure or lack of use in the field. Failure during early field experience will poison attitudes which can only be overcome slowly and at great expense; thus, care must be taken to involve users early on in the design process.

Finally, by their very nature as automatons, computer systems have no inherent ability to recognize their own limitations. When applied in inappropriate circumstances, they will produce answers which may be "logical" but quite incorrect. The entire process, from concept through design, testing, and doctrine development, must include a recognition of this inherent problem. Ultimately, humans must make sound decisions about when and under what circumstances to rely on automated systems.

Vulnerabilities

As the sophistication of the military information systems support structure grows over time, the inherent vulnerabilities will become more important. Planning and doctrine can minimize these vulnerabilities, but they cannot be safely ignored.

First, all military equipment is in danger of capture. Even rear areas are raided to capture or destroy vital elements of important systems. Hence, steps must be taken to prevent equipment loss, to ensure that losses are known, and to frustrate enemy exploitation of captured systems. Unique keys that identify and authorize users on particular systems, devices that report current locations on key hardware items via satellite, authentication procedures, and security codes will be important defensive systems. Doctrine and training necessary to ensure their proper use will also be necessary.

Moreover, DoD's increasing reliance on COTS hardware and software increases vulnerabilities by making military systems familiar to sophisticated adversaries and by exposing them to soft- ware developers and technicians who are not subject to security regulations. Hence, design and acquisition procedures need to consider security and minimize exposure. Indeed, some systems may be too sensitive to rely on COTS designs or procurements.

As the information "grid" is readily available in the battlespace, the system's vulnerabilities will increase because: (a) the number of valid users with access to the system rises, magnifying the "insider" threat; (b) the number of nodes and connection points grows, providing adversaries with more opportunities to penetrate the system from the outside; and if a compromise does occur, the perpetrator will have access to more information than would have been available in the past.

Indeed, as this system grows and becomes more fully interconnected, the mere task of noticing a penetration or penetration attempt becomes extremely difficult. Often system problems cannot be readily diagnosed as "natural" or the product of information warfare attacks. Even a single penetration can be extremely damaging, particularly in a richly connected information system. Obviously, some data (such as concepts of operations, planning documents, and orders) are extremely sensitive. A well-crafted "worm" or computer virus can spread literally with the speed of light once inside a complex system. Moreover, knowing that databases have been penetrated and may be corrupted can be expected to greatly inhibit decisive and effective decision making. New types of defensive decision aids will be needed to detect, assess, and counter such attacks.

C2 Design and Acquisition

Because the inventory of information systems will inevitably continue to undergo rapid development and replacement, the design and acquisition arenas become crucial in the defense against many vulnerabilities and represent an opportunity for proactive postures to prevent or limit exposure.

As they focus on definitive, exhaustive testing against technical, often arcane, specifications, traditional test and evaluation procedures have developed a bad reputation in the operational community, where they are viewed as often preventing the adoption of a "good enough" system. Technology demonstrations have emerged as a way of exposing new systems to operators and operational conditions without having to address arcane testing standards. Reliance on demonstrations alone can be equally unhealthy because it encourages adoption of systems that have not really been tested at all. A more robust, integrated, and operationally oriented process of user assessment, as well as realistic applications (including baselines and benchmarks to ensure new systems add measurable capability) are needed.

DoD's increasing reliance on COTS is having an almost unnoticed deleterious impact on the U.S. Government's in-house capability to maintain the expertise required to adapt COTS systems and create capabilities not needed by the commercial sector. The engineering base required to meet military standards is an essential element of COTS reliance strategy. A coherent program designed to maintain and exercise this capacity is needed. At least part of this program could be devoted to the post deployment support of information systems. In many cases, these systems will need to be revised in order to maintain interoperability with new systems, a process that necessitates the linkage of COTS systems with military requirements. This means not only building linkages between systems, but also having the capacity to "reengineer" the systems and the processes the systems support.

Because C2 systems are never complete and will be continuously undergoing transitions, the ability to maintain mission capability while upgrading or integrating systems remains crucial. This capability requires planning and creativity. The Army's concept of selecting one unit as a "living test bed" for new ideas and equipment and fielding only what is successful in the chosen environment represents one approach to this problem. Other approaches, such as parallel operation of new and old systems during a test period, may be attractive in some circumstances.

Finally, COTS reliance in military systems is very different from relying on commercial systems. Plans for DoD to rely on commercial satellite communications systems must recognize that other clients can make demands on these systems and may limit DoD's access to them in times of crisis. Moreover, commercial services are not always designed for graceful degradation or fully backed up in the event of system failure. Hence, basic "availability" will be an issue when relying on commercial systems, particularly in times of crisis, and needs to be addressed (a) when contractual arrangements are made and (b) when contingency planning is done for crises.

Strategy for Technology Insertion and Utilization

Some remedies can be built into the processes of technology insertion and utilization. Indeed, these remedies represent a crucial line of defense against unintended consequences. The Mission Capability Package (MCP) approach, which permits analysis of each system in the context of the military mission(s) to be supported and encompasses the full range of tools by which problems can be addressed or managed (from technical requirements to training), is the key to success.

Reviewing the extensive lists of concerns identified and the relevant remedies, five action areas emerge: 1) professional military education and training; 2) doctrine, concepts of operation, and command arrangements; 3) technical requirements to perform missions; 4) system design; and 5) organizational issues. In addition, acquisition reform, particularly transformation of test and evaluation from an arcane process to a robust, holistic, and functionally-oriented process, is essential.

Not all remedies are off the shelf. Basic research, applied research, and programs of development will be needed in some areas. For example, defensive decision aids may require basic research. Similarly, decision maker behavior under stress is well understood in the abstract, but may need applied research in a military context before sound design practices can be specified for information presentation and decision support. The tools for realistic training, simulations, and virtual reality programs may need to be developed, although the technologies for them already exist.

Because the unintended consequences of adopting information age technologies are 1) virtually ubiquitous, 2) complex enough to require more than one type of remedy, and 3) involve actions among various organizations that need to be closely linked or coordinated in order to be effective, the orchestration of appropriate remedies into a coherent solution approach is crucial.

To be successful, the approach must allow, even force, those responsible for conceptualizing, designing, developing, and implementing information age technologies to recognize potential unintended consequences and relevant remedies, and to integrate these remedies into existing structures and processes while facilitating the required changes to those structures and processes. This is a tall order.

The stakes here are very high. The major source of adverse unintended consequences is a lack of coherence or a conflict among the different elements of an existing MCP resulting from uncoordinated changes in MCP components. For example, when an organization is provided information that was previously unavailable,

that organization may take advantage of the opportunity for improvement and perform a task differently. This change in behavior could create a conflict in the way the organization relates to other organizations if other adjustments (e.g. doctrine) are not made. Thus, a major advantage of using the MCP approach is that the approach facilitates the early identification of potential conflicts within proposed MCP concepts and provides a mechanism for testing coordinated sets of changes designed to achieve or maintain MCP coherence.

Mission Capability Packages

The MCP approach (depicted in Figure 2) begins with a clearly defined mission or set of missions and seeks to define a) what is required to meet the mission(s) successfully and b) how those requirements may differ from the current force structure, command and control arrangements, organizations, doctrine, and technologies. Solutions, or initial MCP concepts, are developed in the concept development phase based on prior research, lessons learned, and expert judgement. Their strength lies in their thorough-ness and coherence, from a clear mission statement to organizational and force structure, doctrinal approach, and technology needs.

[Image not available]

The MCP approach calls for exposing the MCP concept to review and critique by the operational community and domain experts early and often in order to refine and improve the concept. This review may take the form of demonstrations, experiments, exercises, simulations, modeling, or expert criticism. What matters is that, as the concept matures, the process becomes increasingly focused and that required refinements are incorporated into the MCP. As consensus and supporting evidence emerge, the refinement process is transformed into a development process characterized by a "build a little, test a little" philosophy. Finally, the MCP moves into its implementation phase.

This implementation phase is also comprehensive in nature. Systems may be built, but not in isolation. Doctrine development, command reorganization, relevant professional military education and training, as well as the technical systems themselves, are all specified.

This process has the comprehensiveness, coherence, and orientation necessary to transform ideas and technologies into real operational capability while avoiding adverse unintended consequences. Hence, MCPs are the recommended approach to ensure effective remedies and to minimize risk.

Recommendations

This section deals with the specific initiatives and actions that can be undertaken to ensure that the Department of Defense avoids, mitigates, and manages the unintended consequences of adopting information age technologies. There are a number of opportunities for DoD leadership in this arena. These include providing vision to ensure the community understands the problem and the required types of solutions, articulating particular operational needs, influencing the investments in information systems and their implementation, using joint doctrine to reap the benefits of new technologies while guarding against inherent problems, establishing professional military education and training requirements, and providing an operational perspective on research priorities and the test and evaluation process.

Vision

The vision needed includes a determination to harness and leverage information technologies as an essential part of the requirement to maintain the military strength of the United States in the global arena and to protect against asymmetric vulnerabilities arising from foreign exploitation of information technologies. More-over, this vision should stress the need to tailor systems to missions and to focus attention on mission capability packages as the vehicle for addressing this problem.

Requirements and Investment

Three types of requirements can be identified: operational, technical, and budgetary. Warfighters can and should help shape the requirements for information systems and influence DoD's investments in these by playing an active role in the MCP process. The technical and operational communities need to work much more closely together to develop new MCP concepts and to refine these concepts. Given the set of inertias involved in some components of an MCP, these concepts need to be incubated and nurtured long before the technology reaches the market-place. Defense planners and budgeteers need to think more in terms of MCPs than in terms of individual programs, using MCPs to link programmatic activities needed to implement or maintain an MCP. This would help ensure that all of the necessary components are adequately funded and properly synchronized, thus eliminating one significant cause for an MCP's lack of completeness or coherence.

Joint Doctrine

The doctrine community should be involved at the beginning of the process. When the nature and distribution of information changes, radically new ways of doing business and complications in the old ways of doing business emerge. In many cases, new or modified doctrine can ease or simplify these changes. Changes in doctrine are often essential if the benefits of new information systems are to be realized and inconsistencies between capacity and doctrine avoided.

Involving the doctrine community early will also facilitate the key process of "embedding" doctrine in new systems. Doctrine is being written or changed when decisions are made about who will automatically receive some class of information, who has the work stations from which a database can be updated, or who is able to access and use some class of data. This process needs to be consciously and carefully monitored. Unless the doctrine community is involved, technical personnel responding to technical criteria and standards will be, in effect, making doctrine. If, however, the doctrine community is involved, new systems being fielded will contain and help support current doctrine.

Finally, the movement toward on-line doctrine delivery systems should be supported and rein-forced. The process of doctrine development tends to be slow and cumbersome, in many ways because of the number of people and organizations involved. Automation of the doctrine development and review process will enable simultaneous review at many locations, ease the process of updating or modifying drafts, and enable almost instantaneous distribution of new doctrine publications. Field units could also reduce the paper they maintain if they had global access to publications they use infrequently.

Joint PME and Training

Professional Military Education (PME) must serve as a change agent for the military grappling with the information age. Raising awareness of the threat, opportunities, and vulnerabilities inherent in the changes underway can best be done through the PME structure. If a "teaching hospital" model is adopted so that this new information is conveyed in the context of "real world" experience and actions, the impact can be direct and effective.

While some progress has been made toward bringing PME into the information age, the process needs to be accelerated. This involves changes in the curriculum so that students become current in information technologies (including their advantages, vulnerabilities, limits, and applications) as these impact and are likely to impact military affairs; developing methods of teaching that enable (and require) PME students to become computer literate and knowledgeable of how to obtain information electronically; and developing connectivity within and between PME institutions as well as between these institutions and the simulation and training centers with which they have natural synergy.

Training is perhaps the arena of military affairs where information technology has already had its most profound effect, but also remains an arena where much more can and should be done. Educated military professionals are ready to train on information systems, but these systems must be mastered and their practical limits learned in the more realistic training environment. Moreover, improvements in virtual reality technologies and connectivity provide options for diverse mission rehearsal and training at a fraction of the cost of field exercises. Defining when and where these lower cost training opportunities exist and taking advantage of them must remain a priority. The most cost effective systems will be those that possess embedded training packages and provide near real time feedback, easing the comprehension and retention of lessons learned.

Research and T&E

There is a need for more operationally-oriented command and control research, research that focuses on exploring command concepts and approaches rather than on the technologies that support them.

Another significant contribution can be made to reducing costs, accelerating schedules, and improving the quality of new information systems if the operational, technical, and test and evaluation communities can come together to develop a new approach to T&E. What is needed is an approach that is less "arm's length" and adversarial and is more supportive of an evolutionary design and acquisition strategy.

Currently, the T&E community tends to focus on easily measurable technical standards while avoiding the more difficult task of assessing the operational capabilities and impacts of new systems or their defenses against unintended consequences. Tests are typically pass/fail rather than designed to provide constructive feedback. This approach is more in keeping with traditional acquisition practices than with the evolutionary acquisition processes, adopted more than a decade ago, that have been proven essential in the command and control arena.

Conclusions

A wide range of potential important unintended consequences were identified in the analysis, some representing vulnerabilities, others opportunities that can be exploited if understood, and others that will require or enable new ways of doing business. While these consequences represent challenges, they are changes that cannot and should be neither avoided nor taken lightly. More importantly, those consequences identified can be managed if a coherent, holistic approach, such as the Mission Capability Package, is adopted and pursued energetically.

While systems designers can bypass some problems, the real solutions tend to cluster around PME, training, and doctrine. Success will also require some new knowledge, so both basic and applied research will be needed. Acquisition and T&E reform will also be required if this process is to be fully successful.

Senior DoD management can positively impact the prevention and management of these conflicts by developing and articulating a vision and by demonstrating the importance of these issues through personal involvement and leadership. Mission Capability Packages that ensure linkage between the information systems, the missions for which they are relevant, the needs of the commanders in the field, the force structure, doctrine, training, and education represent the optimal coherent approach.