

Battle-Wise

Gaining Advantage in Networked Warfare

David C. Gompert, Irving Lachow, and Justin Perkins

**Center for Technology and National Security Policy
National Defense University**

January 2005

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE JAN 2005		2. REPORT TYPE N/A		3. DATES COVERED -	
4. TITLE AND SUBTITLE Battle-Wise: Gaining Advantage in Networked Warfare				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) National Defense University Center for Technology and National Security Policy Fort McNair Washington, DC 20319				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release, distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	18. NUMBER OF PAGES 37	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

The views expressed in this article are those of the authors and do not reflect the official policy or position of The National Defense University, the Department of Defense, or the U.S. Government. All information and sources for this paper were drawn from unclassified materials.

David C. Gompert is a Distinguished Research Professor at the Center for Technology and National Security Policy, The National Defense University. Prior to this, he was the Senior Advisor for National Security and Defense at the Coalition Provisional Authority, Iraq. Mr. Gompert has held senior positions at the State Department, the National Security Council, and the RAND Corporation, and in the information technology industry. He has published extensively on international affairs, national security policy, and information technology. His books include *Right Makes Might: Freedom and Power in the Information Age* and *Mind the Gap: A Transatlantic Revolution in Military Affairs*. Mr. Gompert holds a Master of Public Affairs degree from the Woodrow Wilson School, Princeton University and a Bachelor of Science degree in engineering from the United States Naval Academy.

Irving Lachow is a Professor of Systems Management at The National Defense University and Director of the Information Resources Management College's Advanced Management Program. Previously, Dr. Lachow was a Senior Associate at Booz Allen Hamilton, where he managed projects in the areas of IT Strategy and Planning for numerous government clients. Dr. Lachow has extensive experience in both IT and national security. He has worked for Digital Signature Trust, the RAND Corporation, and the Office of Deputy Under Secretary of Defense (Advanced Systems & Concepts). Dr. Lachow received his Ph.D. in Engineering & Public Policy from Carnegie Mellon University. He earned a B.A. Political Science and a B.S. in Physics from Stanford University.

Justin Perkins is a Research Associate with the Center for Technology and National Security Policy, The National Defense University. Before working with NDU, he served as COO for World Blu, Inc., a consulting firm pioneering the field of organizational democracy, and as co-founder and director of Afrique Profonde, a human rights organization in Congo. He also has been involved with several small businesses and served for several years as a water resources administrator for the State of Colorado. Mr. Perkins holds a Masters of Business Administration from the University of Colorado and a B.A. in History and World Perspectives.

Defense & Technology Papers are published by the National Defense University Center for Technology and National Security Policy, Fort Lesley J. McNair, Washington, DC. CTNSP publications are available online at <http://www.ndu.edu/ctnsp/publications.html>.

Contents

Introduction.....	1
Networking in Warfare: End or Beginning?	2
Exploiting Information in Messy Conditions	3
Battle-Wisdom	6
The Military Networking Monopoly Will Not Last	12
China	13
Al Qaeda	14
Adapting to Networked Adversaries.....	16
Improving Cognitive Performance in the Civilian World	20
Building a Battle-Wise Military.....	23
Developing the Individual.....	23
Reforming Command and Control.....	28
Developing Intelligent Teams.....	30
Suggestions	32
Conclusion	34

Introduction

From fighting terrorists to stabilizing a war-torn country to waging all-out combat, military campaigns are increasingly shaped by networks that enable dispersed and disparate forces to collaborate by sharing data. Along with the high-precision sensors and weapons they connect, networks are turning information power into military power.¹ Defense investment priorities are shifting from mechanized platforms and weapons to the information collectors, processors, links and services that compose these networks. With its unmatched defense resources and technological talents, the United States has pioneered networked warfare. But the United States will have company—not all of it friendly. For example, China and Al Qaeda, using very different doctrines, are showing interest in tapping the power of information. Indeed, Al Qaeda and its franchised affiliates are displaying cunning and resourcefulness in putting this power to work with virtually no investment.²

As adversaries exploit networks, the United States must seek new leverage by improving its fighters' ability to use information in war's confusing, critical, and violent conditions.³ Blessed with more, better, and timelier information, yet vexed by increasingly murky circumstances, the cognitive faculties of military decisionmakers—lieutenants no less than lieutenant generals—are more crucial than ever. In a forthcoming National Defense University book, the authors suggest why and how U.S. and allied forces should improve these faculties to attain new operational and strategic advantages, or at least to avoid the loss of the advantages they now enjoy. Although military combat is unique, the authors draw lessons from non-military sectors, including some in which urgent life-and-death decisions must be made. This paper summarizes their thinking.

While this is neither the first nor the last word on why and how to gain cognitive advantage, it aims to take an integrated view, provide a geo-strategic context, broaden and heighten awareness, frame policy issues, offer preliminary advice, and indicate where research and analysis is needed.

¹ We will use “network” in its broadest sense, to include not only information processing systems and communication links but also the platforms, sensors, command centers, and troops themselves that make up a force. While improved precision of individual sensors and weapons, owing to information technology, account partly for the enhanced effectiveness of a force, their precision is increasingly both enhanced and exploited by networks.

² Rohan Gunaratna, *Inside Al Qaeda: Global Network of Terror* (New York: Columbia University Press, 2002).

³ Throughout this paper we will refer to warfare, combat, and military operations more or less interchangeably. Of course, military operations span a broad continuum, including counter-terrorist actions, peacekeeping and humanitarian relief. We are convinced that both information networking and improved cognitive performance offer benefits across this continuum. Indeed, operations against non-states and in semi-permissive and permissive conditions may be fraught with ambiguity and confusion, even if not at the levels of danger and urgency found in fighting the armies of other states. The cognitive demands of non-combat operations are different than those of combat but nonetheless formidable, growing and in need of the same attention. Thus, the thrust of this paper can be applied to combat and non-combat operations alike.

Networking in Warfare: End or Beginning?

The network is the latest leap in how humans fight. Since warfare began, every favorite weapon has sooner or later been outdone by a better one. Clubs could defeat fists but were in turn defeated by spears and arrows, which then succumbed to guns and bombs. With industrialization, placing guns and bombs on mechanized vehicles, such as tanks, submarines, and airplanes, brought decisive advantages in mobility, range, survivability, and explosive force. Those who mastered the production and use of each new technology have held at least a temporary strategic edge over stragglers, as Britain did on the high seas in the 19th Century, Germany did on land by the outset of World War II, and the United States did by the end of World War II and again by the end of the Cold War.

We have reached the point where forces with information links among mechanized platforms, high-precision weapons, advanced intelligence collectors, well-trained fighters, and able decisionmakers can make quick work of modern but non-networked mechanized forces. The swift trouncing of Iraqi Army and Republican Guard divisions by smaller but networked American and British ground, air, and surveillance forces in Operational *Iraqi Freedom* marked the passing of the age of 20th Century warfare.⁴ Such connectivity, wisely used, can also improve military performance in non-combat operations, such as peacekeeping and humanitarian relief.⁵ By enabling any part of a force to operate with any other part, networking affords not just unprecedented capability but unbounded opportunity. It has been called the “apotheosis of conventional warfare.”⁶

Whether or not networking represents the “end of military history,” there will be a scramble among nations and groups to exploit it, much as advances in propulsion unsettled rather than settled warfare in the mid-19th Century and as radar triggered efforts to exploit remote detection in the mid-20th Century. As more armed forces exploit information technology and embrace networking in the years to come, some perplexing questions will arise: If two belligerents have networked forces, how can one gain an edge over the other? Are the platforms of both belligerents more vulnerable because networked sensors can see them or, instead, less vulnerable because they can be dispersed? How can information be put to the fullest use and best effects? What is the next defining, decisive military capability? Of immediate interest, in view of persistent insurgency in Iraq, how can networked forces be used to defeat an irregular enemy dispersed and hidden in a civilian population?

The answer to this line of questions, we believe, is right between our ears. The capability that can make the most use and sense out of information—indeed, has biologically

⁴ U.S. and allied forces had many advantages, including superior equipment, firepower, quality, discipline, and doctrine. However, what accounted for the remarkable speed of victory for a comparatively small force was the awareness, integration, and precision afforded by information systems and networks.

⁵ David C. Gompert, Hans Pung, Kevin A. O’Brien, and Jeffrey Peterson, *Stretching the Network: Using Transformed Forces in Demanding Contingencies Other Than War* (Santa Monica, CA: RAND, April 2004).

⁶ Martin Libicki and James Mulvenon, *Dialectic Militarism* (Santa Monica, CA: RAND, forthcoming).

evolved to do so—is the human brain. As we shall discuss, the mind is the key to graduating from information superiority to *time-information* superiority, even as enemies adopt networks—indeed, especially as they adopt networks. The erosion of the American monopoly in harnessing information technology for military purposes, which has already begun, creates a need to define, gain, and hold a lead in the ability of soldiers to think soundly and quickly in threatening and confusing situations. This explains the growing buzz in defense research and policy circles about the cognitive implications of “net-centric warfare.”⁷

There is, of course, nothing novel in the idea of superior minds winning battles. Brilliant generalship has always mattered, sometimes more than force strength. Lee outfoxed Hooker at Chancellorsville. Eisenhower’s D-Day plan befuddled the Wehrmacht’s best generals. In Vietnam, Giap got the better of Westmoreland et al. But networking offers more: an unprecedented opportunity to prevail in battle by bringing to bear more brainpower—not just brainier generals—by permitting better problem solving on the part of the individual, by mobilizing more minds, and by honing the collective intelligence of whole units and teams.

While information networks can help military organizations and challenge military personnel in many ways, the concern here is with operations—mainly but not exclusively warfighting—and with those who conduct them. Of course, networks alone will not ensure that the warfighters connected to them will make full use and good sense of information. That will take a purposeful strategy of its own.

Before sketching such a strategy, it is helpful to consider:

- the changing demands of problem solving and decisionmaking in warfare;
- potential threats that make it crucial for U.S. forces to meet these demands;
- the cognitive abilities that will matter most in operating against these threats; and
- lessons about cognitive effectiveness from non-military experiences with networks and decisionmaking.

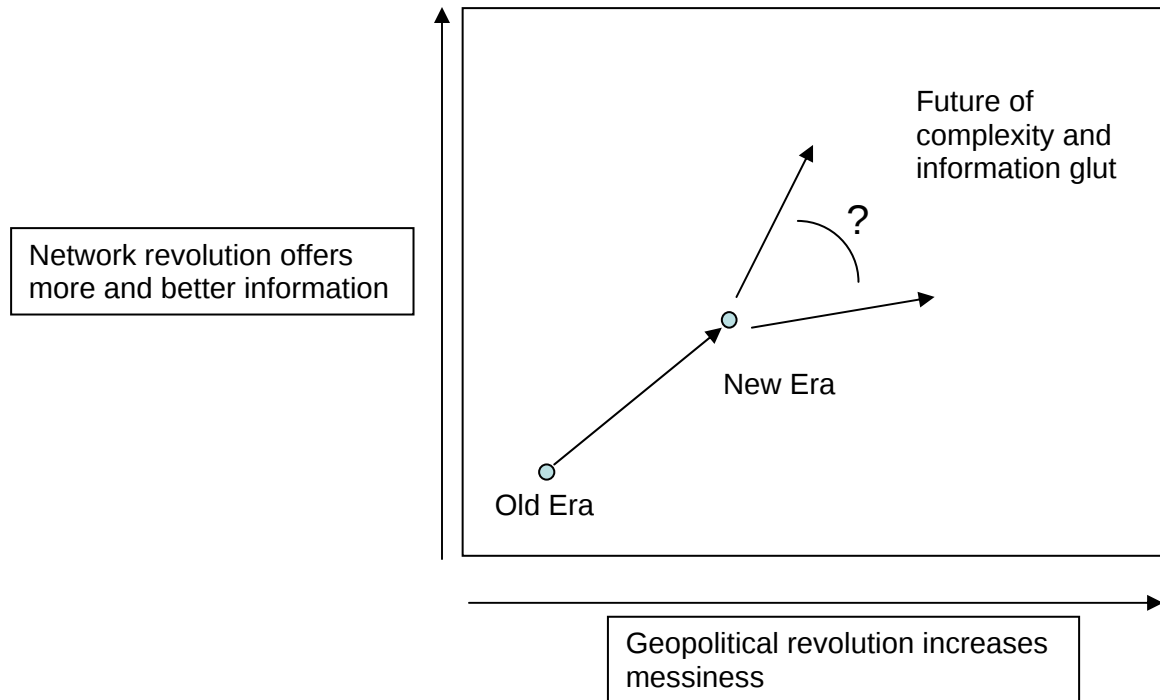
Exploiting Information in Messy Conditions

The global security environment has changed in two fundamental ways over the past fifteen years or so. First, technologies spawned by the information revolution can now deliver data of unprecedented volume, quality, and speed to those forces that apply network principles in the way they organize and operate. Second, with the end of East-West confrontation, geopolitical upheaval is causing continuing turbulence and unpredictability at global, regional, and local levels. As figure 1 suggests, it is uncertain which effect will be stronger in the future, the clarity resulting from more and better information via networks, or the complexity caused by increased turmoil. The interplay

⁷ For example, see the Defense Advanced Research Project Agency, “Improving Warfighter Information Intake Under Stress” project, available at <http://www.darpa.mil/ipto/programs/augcog/>, and Martin Burke, *Thought Systems and Network Centric Warfare*, available at <http://www.dsto.defence.gov.au/corporate/reports/DSTO-RR-0177.pdf>.

of these two revolutions is complicated by the fact that plentiful information, unless properly organized, can aggravate rather than ameliorate complexity.

Figure 1: Interplay of Two Revolutions



Even before these dual revolutions, making reasoned and timely decisions in the violent crush of warfare has been a challenge. The history of military misjudgments—hopeless head-on assaults, failure to heed clear warnings, unwarranted caution, lost opportunities—rivals that of human shortcomings in any field. The heart of such difficulty is that people are not very good at solving complex problems rationally.⁸ Their reasoning relies on cognitive models that, of necessity, simplify reality, especially the causes and effects of so-called “dynamic systems” (like wars and child-raising). The more complex the problem at hand, the wider the gulf between reality and the model of reality formed and used by the mind to grasp and solve such problems.

If, in general, humans are not good at solving complex problems rationally, they must be severely handicapped at doing so during war, when stakes are high, clarity is elusive, time is short, and a mortal enemy shares the battlefield. Not surprisingly, research shows that decisions in combat, as in other intense and urgent circumstances, tend to be made intuitively⁹—drawing on experience, often tacitly, and going with familiar solutions—rather than by analyzing and comparing the costs and benefits of multiple options. While intuition can complement explicit, structured reasoning in problem solving in many

⁸ Herbert A. Simon, *Administrative Behavior* (2nd ed.) (New York: Macmillan, 1957).

⁹ Intuition is defined as the power or faculty of attaining to direct knowledge or cognition without evident rational thought and inference.

situations, it is especially important when the time for such reasoning is severely compressed. Therefore, the capacity for consistently sound intuition can differentiate good warfighters from less good ones and seasoned warfighters from novices.

At the same time, complex military-operational problems can cry out for reasoning.¹⁰ It is normally better, time permitting, to acquire more information, apply logic, and conduct analysis, if only to buttress intuition. After all, the reason to rely on intuition is urgency, not a belief that experience is unfailing or that added data and careful reasoning are generally superfluous. Reasoning in warfare also is important because the fluidity of global security conditions may reduce the applicability of experience and, thus, the reliability of intuition. Confidence in experience and so-called pattern-recognition must be tempered by the realization that the conditions and conduct of warfare have become highly fluid, non-repetitive, and unfamiliar.¹¹ What worked in the Gulf War did not much apply in Bosnia; the Kosovo campaign did not provide a template for Afghanistan; the way Baghdad was taken in 2003 offered few pointers for battling Iraqi insurgents, militants and terrorists in 2004; and block-to-block fighting in Fallujah will not prepare U.S. forces for a confrontation with Chinese forces in the Taiwan Strait.

Chances are slim that a given soldier heading into a given military contingency will have had analogous experience. Of course, experience can be shared, in effect, by training. However, insofar as training is predicated on the variety of problems that forces *have faced*, its value will be reduced if the next decade is unlike recent ones. For this reason, new training methods are needed—in fact, are being tried—to bolster decisionmaking despite systemic and situational turbulence. (More on this later.)

Even as change and uncertainty may weaken the reliability of intuition, the quickening speed of warfare may shorten the opportunity for reasoning. Depending on circumstances, there may not be enough time or information to evaluate and compare options before acting. The value of well-managed networks is that they can increase the quality, amount, clarity, and promptness of information and the possibilities of collaboration available to the decisionmaker. While they may not improve our mental models, networks augment them efficiently by offering a more faithful, complete, and timely view of reality, as well as added options for action.¹² In sum, if a messier world demands better military reasoning, networks facilitate it.

¹⁰ Reasoning is defined as the power of comprehending, inferring, or thinking, especially in orderly and rational ways.

¹¹ We do not discount the school of thought that pattern recognition can be valuable. Rather, our point is that when each contingency differs significantly from previous ones and is itself continuously changing, recognition can be severely challenged and cannot be counted upon.

¹² Because networks may also confuse by providing a glut of information, we must look to improvements in information management to help ensure, through filters, displays, and other techniques, that more data truly informs. In addition, the principle of smart-pull should reduce unwanted and unhelpful information, in the eyes of the beholder. By aligning information management with the demands of the smart user, networks themselves can be made “smarter” in the sense of being designed and operated to be more discriminating and useful regarding what and how information is made available.

The right formula for improving cognitive performance in 21st Century warfare, generally speaking, is a combination of more *timely reasoning* and more *reliable intuition*—the former to make use of networked information and the latter to offset the decline in the utility of experience. More than a combination, new conditions call for the integration of reasoning and intuition into a sort of savvy-yet-thoughtful quality we call *battle-wisdom*.¹³ Battle-wise individuals, teams, and forces can create time-information advantages by making swift but sound decisions in the heat and fog of combat. Moreover, the way in which military-operational decisions are taken can be reformed to integrate intuition and reasoning and, thus, exploit battle-wise abilities.

Battle-Wisdom

The battle-wise soldier is in a unique position to fuse two sources of knowledge:¹⁴ data that he or she pulls from whatever is posted on the network; and immediate, if tacit, awareness of what he or she is experiencing. This assumes that the soldier, whether a small-unit commander or a joint-force commander, has ready access to all information posted on the network that could be of value in addressing the problems at hand. Consistent with the “smart-pull” principle, on which the Internet is based, users can draw information they think might help them solve the problem before them. Because they are directly involved, and assuming they are perceptive and well prepared, users have a better idea of the information that could benefit them than some distant headquarters staff or others who post data on the network.¹⁵

This power of distributed cognition¹⁶—with the warfighter sensing the situation, then pulling relevant information from the network—argues for decentralizing decisionmaking authority. It also indicates a conceptual shift from *network-centric warfare* to *warrior-centric network*. This shift would have several advantages. First, it would underscore the tenet that the truest measure of any network’s worth is the level of service to and satisfaction of its user(s). Second, it would imply that flexible, horizontal collaboration among warfighters is an option of growing importance, not readily available when communications could support only vertical command and control. Third, it would make explicit that the highest power of information is the enablement of people.

Realistically, it is far harder to satisfy via smart-pull from a network the information needs of a warfighter than those of an Internet user. Knowing what information to post on the network in the first place implies knowing all facets of all predicaments and opportunities a warfighter—for that matter, *all* warfighters—may face and, thus, what information might be helpful. Moreover, the warfighter will not be aware of all the relevant information that could be pulled, and the prospect of the commander of a unit under surprise attack having to “browse” the operations network for useful information is

¹³ Battle-wisdom is the ability to decide and act in urgent, complex, high-stakes situations through well-developed self-awareness, intuition, reasoning, and leveraging of networks.

¹⁴ Knowledge is defined as the fact or condition of knowing something with familiarity through experience or association.

¹⁵ David S. Alberts and Richard E. Hayes, *Power to the Edge: command and control in the information age* (Washington, DC: CCRP Publication Series, 2003).

¹⁶ Cognition is defined as the act or process of knowing including both awareness and judgment.

neither comforting nor realistic. For a local decisionmaker to have superior information will require a good deal of investment in network development and information management (IM).¹⁷ Nevertheless, the goal and the general direction toward it are clear.

Meanwhile, senior commanders increasingly have remarkably detailed and comprehensive information displayed before them. Whether they have enough confidence in subordinates to delegate authority and enough self-discipline to resist micro-management remain important open questions. Of course, confidence must be deserved. The subordinate must be willing to take responsibility for the consequences of his or her decisions—that is, to be a leader-in-action, if not in hierarchical order. Moreover, until enough tactical-level officers are sufficiently battle-wise to make good use of the information from the network, senior commanders will understandably be reluctant to delegate and be tempted to micro-manage. For tough decisions, a good leader would rather risk making a mistake and suffering the consequences than having a subordinate do so. While other military cultures—the British, for instance—have long stressed decentralized operational decisionmaking, U.S. senior officers will likely set the bar high for battle-wise juniors to earn such authority.

To illustrate these factors, imagine a motorized column of peacekeepers ambushed as they move through a remote province of an African country engulfed in tribal violence. Imagine that this unit is networked for this mission with other nearby patrols, sensor-carrying drone aircraft, an attack-helicopter unit, a provincial operations coordination center, force headquarters, and an intelligence fusion facility. Now visualize the major (he, in this case) in command of the ambushed column being not at the network's extremity but at its center. Assume, for our purposes, that good IM is in place, and that this battle-wise officer is trained to know what information to pull from the network, including intelligence about the threat, the latest data on the non-combatants he has been sent to rescue, weather reports, and information about the availability of back-up forces.¹⁸

Senior officers up the chain of command have confidence in the major and appreciate that he has a fuller immediate view than they of unfolding events. Therefore, within the unit's stated mission and rules of engagement, the major has the authority to decide how to respond and what support to call. If it is possible that the major's decision could jeopardize not only his own unit and mission but also the larger operation or other units,

¹⁷ Although a full discussion of IM is outside the scope of this essay, it is obviously crucial to cognitive effectiveness. IM in military operations is anything but straightforward. Even "smart" users' attempts to pull information from the network are hindered by their chaotic, messy conditions and time-constraints. To be effective in operations, IM must take account of the decisionmaker's predilections, culture, and needs, and it must be updated when the threat changes. Even then, the value of data can be limited without the context of a problem—and the context of military operations is hard to foresee. Finally, the effects of IM vary with the decisionmaker's experience. Experienced individuals know what information to select, organize it well, recognize when something is missing, and adjust decisions to compensate for incomplete information.

¹⁸ Though it may take years before the network can meet a user's information needs, this is still a fair assumption.

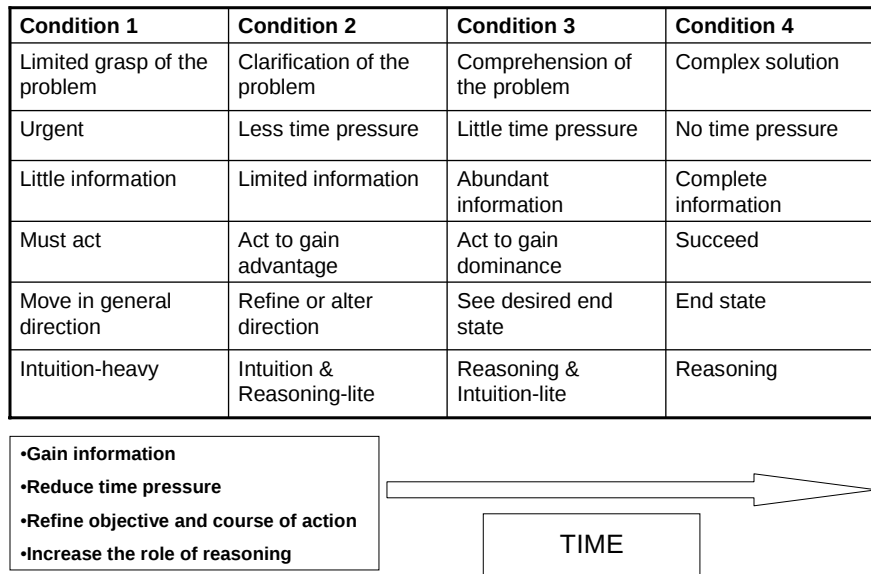
an over-riding decision by higher command might be indicated.¹⁹ This will often be the case, given the ease and speed with which word of the unit's fate is shared with the outside world. But let's assume here that the major's chosen course of action, whether right or wrong, will not have serious ramifications beyond his unit and its results. He is thus inside his envelope of discretion.

Depending on what the major senses from the immediate situation and summons from experience (including his training, of course), his initial choice may be simply to hunker down or to pull back. His intuition may tell him that the option of attacking the ambushing forces is out of play because his experience and mental model suggest that an inferior enemy force would not have attacked him. Once he has more data—from all sources accessible via the network—about the threat, the presence of innocent civilians, and the time it will take to be reinforced, the major can weigh and decide among several options: to engage in a fire-fight, to break off and wait for reinforcement before engaging, to retreat, or to slip the ambush and proceed to carry out the original assignment. In sum, while he may get advice from headquarters, the major is best placed to determine what is happening, what information is needed, what help is needed, what options are available, and what risks exist. The critical question then becomes how, and how well, he selects the best course of action. While vital, intuition will get the officer only so far before he must analyze all available information and weigh his options.

Both intuition and reasoning are indispensable in overcoming the pressure, urgency, and messiness of warfare in the information age. When facing an unexpected threat or opportunity, initial action may be based on what experience says will work, but should also aim to increase both information and time. As this action clarifies conditions and buys time, structured reasoning is made possible, leading to a refined or revised course of action after examination of options. Eventually, with time and information now on the decisionmaker's side, sound and superior reasoning can lead to success. Of course, it may be that the major's initial intuition prompts him to take what proves to be the best course of action, in which case added time and information will provide validation. This decisionmaking process is depicted in figure 2.

¹⁹ In traditional terms, it may be helpful to think of the major's decision domain as being at the tactical level, whereas his superiors are responsible for the operational and strategic levels. While these value of these distinctions is being eroded by complexity and networking, they still adequately connote the levels at which decisions should be made.

Figure 2: Battle-wise Decisionmaking Process



The key to integrating intuition with reasoning is the “self-awareness” of the decisionmaker.²⁰ Knowledge of one’s mental models and their limits can answer the question: does my past experience apply or not to the situation I face? If the answer is that past experience applies, intuition might be a reliable basis for response. But if there is no suitable mental model, more information should be sought, organized and analyzed before making a decision.²¹ Even then, time can be borrowed by a provisional, intuitive decision aimed at least partly at getting better information.

We do not presume that such decisionmaking is easy. Because people who need to act with little time naturally rely on intuition over reasoning, conscious intervention is needed to avert mistakes when intuition is inadequate or worse misleading. The individual must be able to determine objectively whether his or her stored models apply. Such discipline and dispassionate self-awareness are hard for most people (which is why they must be developed). Still, verbalizing a simple question—is my experience applicable or not?—can result in appreciably better decisions under time pressure.

In the case of the ambushed major, his self-awareness established that intuition was reliable enough to tell him not to attack, but only that. Identifying, weighing, and

²⁰ Self-awareness is defined as consciousness of one’s individuality, including the strengths, weaknesses, range, and limits of one’s cognitive abilities.

²¹ We draw here loosely from a growing body of work on adaptive planning. See Robert J. Lempert, Steven Popper, and Steven C. Bankes, *Shaping the Next One Hundred Years: New Methods for Quantitative, Long-Term Policy Analysis* (Santa Monica, CA: RAND, 2003). Whereas their work deals with long-term planning and decisionmaking, we advance the proposition that this way of solving problems may be compressed into operational time-frames.

selecting among options beyond “don’t attack” required more information and more time, which he gained by holding his ground. In other words, his intuition was reliable enough to yield a good-enough initial step and give him the time to pull crucial information from the network to aid in making a more reasoned decision.

Military combat is not the only domain where complex, life-and-death problems must be solved by people with insufficient time to analyze their options. We can learn about both cognitive qualities and decisionmaking from examples of people combining intuition with reasoning in non-military settings.²²

For instance, neo-natal intensive-care wards regularly present nurses and doctors with split-second choices that determine the survival of premature babies. Neo-natal nurses must know how to detect an infection called sepsis that can cause death if not spotted immediately. A set of symptoms presents visual cues that neither instruments nor nurses who have not previously witnessed the symptoms can readily detect. Any of these—change in skin hue, temperature, lethargy, swelling—might and often does appear alone for other reasons and without consequence. However, it is their combination that one must recognize.²³ In one case, a rookie nurse on duty failed to perceive the indications of sepsis in a baby in her ward. The nurse’s supervisor happened by and immediately noticed that something was not right about the baby, without having seen it before. The supervisor quickly looked at the instrument readings to check and augment her intuition. The baby was treated, and a day later tests confirmed the validity of the nurse’s decision. Her ability to integrate intuition and analysis with no time to spare saved the baby.²⁴

Forecasting violent weather poses demands of complexity and urgency that rival those of warfare. Extreme weather is often highly complex, dynamic, surprising, and, of course, dangerous. The best forecasters tend to rely first on their intuition before using data from their instruments and networks. They check the dew on the handrails as they leave home in the morning, notice their footprints in the grass, sense the temperature of the air, and of course look at the clouds. They register all this and then apply mental models from their accumulated understanding of patterns and correlation of variables. Upon arriving at work, they examine the latest data. Their intuition enables them to look for a story in the data, to search for anomalies and to come to a conclusion rapidly. Their self-awareness warns them if their intuition may be weak in any given case. They must be able to pull whatever data they need, form mental simulations of what might be unfolding, develop a thesis, form judgments as they gain confidence in their understanding of current reality, and adapt their judgments as they get new information.²⁵ Weather-wise forecasters are the meteorological equivalent of battle-wise soldiers.

Experience, intuition, and pattern-recognition worked in both of these examples. But it took processing of information from instruments and networks before the nurse and the

²² These examples are drawn from Gary Klein, *Intuition at Work: Why Developing Your Gut Instincts Will Make You Better at What You Do* (New York: Random House, 2003).

²³ *Ibid.*, 7.

²⁴ *Ibid.*, 8.

²⁵ *Ibid.*, 250.

forecaster could make definitive judgments about a baby's precious life and the course of a violent storm. The combination of intuition and reasoning permitted them both to cope with complexity quickly.

The most precious commodities in situations of urgency and complexity, like warfare, are time and information. Yet they tend to work at cross purposes: the greater the haste, the less chance one has to collect data and to reason, thus forfeiting the benefit of information technology. Lack of time means lack of information, and lack of information means dependence on intuition and experience, which may not be appropriate or sufficient to the problem at hand. Although usually tolerable in routine life, this time-information problem must be overcome when lives depend on solving complex and unfamiliar problems. Information networks (and IM) can furnish usable data quickly. Self-aware nurses and weather forecasters succeed by integrating intuition and reasoning to exploit information expeditiously. They also have authority to make judgments on the spot and are willing to take responsibility.

Because of the changing global security environment, the U.S. military must expect no less of networked warfighters.

The Military Networking Monopoly Will Not Last

If networking makes it possible for U.S. forces to nurture battle-wise people and decisionmaking, and the messiness of the new landscape makes it important to do so, the adoption of networking by opposing forces makes it absolutely essential. It is only a matter of time before any number of other states and even non-state groups, some hostile, use networking technologies and concepts. Although they may be technologically far inferior to U.S. forces in firepower and networking, they can still alter the course and odds of warfare. The mutation of Al Qaeda and the insurgency in Iraq in the past year provides a glimpse of what U.S. forces will face in the future. Precisely because networking is so flexible, information so powerful, and information technology so accessible, U.S. complacency would be negligent.

The classic conditions for the breakdown of a monopoly are that the lucrative returns of the monopolist's commanding position attract would-be competitors, and that barriers to their entry are low. As the stories of the iron-clad ship, the tank, the aircraft carrier, and nuclear weapons show, military monopolies are in this respect no different than market monopolies.²⁶ Where networked warfare is concerned, the first condition—lucrative returns—is clearly met. If the success of the initial U.S. combat operations in Afghanistan and Iraq has not caught the attention of potential adversaries, the transforming role of information networks in many other human endeavors, including the Internet, surely has.

Barriers to entry, the second condition, are lower than we may have expected. The spread of the Internet and other applications of information technology suggests that it is unnecessary to be able to invent or produce information systems and services to use them adeptly and strategically. Companies that are proficient at using information technology—banks and distributed retailers, for instance—are often unskilled, even uninterested, in what it takes to make it. And we all know talented users who have no clue about how computer networks work, let alone how they are built. The spread of accessible information technology, infrastructure, and services will continue apace. Steadily declining prices, reflecting declining production costs and fierce competition, have sustained a buyer's market for information technology and hastened its diffusion. As standardized information products and services become commodities and utilities, affordability will remain a non-problem.

Potential enemies watch the United States network its forces. They read the literature and check out the web sites. They know which commercial-off-the-shelf products and services are adequate for their purposes. They need not do research and development, with all the attendant costs, mistakes, and dead-ends. Being uncompetitive at the creative front-end does not preclude success as the technology is productized, commercialized,

²⁶ In some cases—notably, French leadership in designing tanks and German superiority in using them—the challenger, or follower, has even been “first to market.”

copied, and distributed.²⁷ The very nature of this technology shortens the time between discovery and widespread application—it communicates the know-how that allows its use. Because data-networking is proven, the leverage of followers is growing. Because it is ubiquitous, free-riders abound.

Thanks to easy access to global information technology markets, services, and infrastructure, countries such as China and Iran and terrorist groups such as Al Qaeda can network their forces and fighters for their own purposes. As they do, their forces will become less vulnerable to and more capable of locating and striking U.S. forces, even though the latter remain much stronger and better networked. While the United States can respond by attacking the information systems and links of its adversaries, they can gain considerable protection by using generally available infrastructure and services, especially if anonymous or undetectable.

China

China has considerable and growing capabilities in information technology and networks, owing largely to foreign technology transfer for the purpose of gaining access to China's cheap labor and vast markets. The Beijing regime has been ambivalent about the use of information technology within the country, fearing it could stir up and spread dissent. However, while the government may continue to try to block what it sees as seditious Web sites, it will not, and largely cannot, block the technology from spilling into and throughout the country.²⁸ In addition, the Chinese have shown interest in acquiring commercial networks that extend throughout the region.²⁹ They seem to have made the acquisition and exploitation of information technology a matter of national strategy. While this surely has economic motivations, there are also signs of interest in adapting information technology and networking for military use.³⁰

The Chinese face high institutional and cultural hurdles in military exploitation of networking, such as inter-service blockages and reluctance to decentralize command and control. However, a new generation of Chinese military officers, like many young Chinese businesspeople, understand and want to harness the power of information.³¹ We must assume that the Chinese will apply networking increasingly, if selectively, in operational and force planning. More than an assumption, we know that the Chinese are already investing in extended-range surveillance systems—including the use of the European “Galileo” space-based global positioning—which will of course be networked with Chinese forces.

²⁷ This may be different from previous technologies, in which familiarity with their science and production afforded prolonged advantages in use.

²⁸ Michael Chase and James Charles Mulvenon, *You've Got Dissent: Chinese Dissident Use of the Internet and Beijing's Counter-Strategies* (Santa Monica, CA: RAND, 2002).

²⁹ Robert C. Fonow, *Beyond the Mainland: Chinese Telecommunications Expansion*, Defense Horizons Number 29 (Washington, DC: Center for Technology and National Security Policy, July 2003).

³⁰ Martin Libicki and James Mulvenon, *Dialectic Militarism*.

³¹ Ibid.

Strategically, China's aim is to deny the United States the ability to control East Asian waters, which surround some of the world's most important states and economies. China's strategy of developing the capability to take Taiwan, even if only to strengthen its negotiating hand, has focused its military planning on neutralizing U.S. capabilities to come to Taiwan's rescue. Beyond the Taiwan problem, Beijing will likely find increasingly intolerable U.S. policies and forces that are meant to constrict China's littoral military activities and to preserve unrivalled U.S. freedom of action and influence. The Chinese may also feel compelled to lengthen their military reach sufficiently to protect sea lanes and choke-points, e.g., in Southeast Asia, through which increasingly vital oil imports are shipped.

The superiority of U.S. forces notwithstanding, the networking of Chinese forces could present a new situation. In general, networking provides three core benefits: (1) enhanced *awareness*, thanks to the ability to fuse and disseminate the product of an array of networked sensors; (2) greater *precision* in sensing and in weapons effects, thanks to target-location and weapon-guidance information available via the network, e.g., from GPS; and (3) the ability to *disperse* force elements while managing them as a coherent force and concentrating their effects, thanks to broadband communications. If each of two opposing forces enjoys all three of these benefits, its ability to operate while dispersed could be offset by the other's ability to find, target, and destroy its forces with precision. The net effect, theoretically, is that *both* forces would be more vulnerable than if opposed by non-networked forces, though not necessarily equally vulnerable. Even the superior and better networked of the two forces would be more exposed—unless and until the inferior force was decimated—which could alter the costs and course of combat.

In the case of Chinese and U.S. forces, this would not mean parity in vulnerability or in warfighting power. Even after linking up long-range sensors, with air, naval, and missile capabilities and command and control, Chinese forces would remain far behind American forces in battlefield awareness and operational integration. Keep in mind, however, that Chinese forces are currently highly vulnerable and U.S. forces are not at all. Insofar as networking permits dispersing forces, thus reducing their vulnerability, the effect of Chinese networking would be to make Chinese forces at least somewhat *less* vulnerable and U.S. forces somewhat *more* vulnerable than they are now—a potentially significant shift with strategic implications in one of the world's most vital regions. As China deploys and networks more and better sensors and precision weapons, the efficacy of U.S. intervention against Chinese forces could decline.³² While this would not give China unchecked power-projection capability, it could give China a freer hand to influence East Asian developments, possibly including the fate of Taiwan.

Al Qaeda

Al Qaeda has no tanks, fighter aircraft, or frigates—no forces to be destroyed the way Iraq's were. Nor does Al Qaeda have overhead sensors capable of tracking U.S. forces.

³² The fielding of long-range surveillance capabilities may be the "long-pole" for the Chinese, since without them their forces, however well networked, will be blind to U.S. forces beyond coastal waters. The Chinese know this and are investing in space-based and other sensors.

Since the destruction of Al Qaeda strongholds in Afghanistan by networked U.S. forces, and Osama Bin Laden's escape from Tora Bora, Islamic terrorists have shunned reliance on large fixed concentrations. Al Qaeda relies on webs of people, not military platforms, and people are hard to find and identify without using other people as infiltrators or informants, which is not easy against wary terrorists.³³ Networks enable Al Qaeda to be more fluid, flexible, elusive, and strategic. Al Qaeda may become to low-capital networking what the U.S. military is to high-capital networking. And it may be institutionally more adaptable—a “quicker study.”

Al Qaeda will not exploit networking as traditional military forces do. Thus far, while the evidence is mixed, it seems that Al Qaeda has not evolved into the sort of peer-to-peer network that facilitates collaboration and synchronized attacks without central direction. Rather, its form has been cellular, under central direction, and with the cells not connected with or necessarily aware of each other. However, as it metastasizes and as its original leaders loosen—or are forced to loosen—control, Al Qaeda could become a distributed, fluid, and self-organizing mass of planners, fighters, financiers, and propagandists—some networked, some not—under one brand name. In any case, already its exploitation of networks would be enviable were it not so evil.³⁴

Al Qaeda's “use of the Internet and videotapes demonstrates that ‘perception management’ is central to the conduct of its war with the West.”³⁵ It does not need dedicated information infrastructure or costly special services. Al Qaeda uses public networks for propaganda, recruitment, training—its own malevolent distance learning—fundraising, coordination, and targeting. Its “use of the Internet through web sites, email, message boards, and chat rooms allows dispersed members to stay in touch constantly, while maintaining the operational security and compartmentalization demanded by their work, under cover of the Internet's anonymity.”³⁶

Being both distributed and hunted, Al Qaeda takes communications security very seriously.³⁷ It uses encrypted, anonymous, and other non-detectable communications, making interception quite difficult.³⁸ Insofar as Al Qaeda is able to operate effectively as a highly distributed organization, its vulnerability to a single knock-out punch is reduced.³⁹ Don't count on anything as convenient as another shoot-out between U.S. and concentrated Al Qaeda forces. Consequently, sophisticated international networks of intelligence and investigative capabilities, infiltration, speed, stealth, and skilled police or

³³ Martin C. Libicki and John D. Woodward, “Biometrics and the Feasibility of a National ID Card,” in John D. Woodward, Nicholas M. Orlans, and Peter T. Higgins, *Biometrics: Identity Assurance in the Information Age* (New York, McGraw-Hill, 2003).

³⁴ See “The Terror Web,” Lawrence Wright, *The New Yorker*, August 2, 2004.

³⁵ Institute for Security Technology Studies, *Examining the Cyber Capabilities of Islamic Terrorist Groups*, available at https://www.ists.dartmouth.edu/TAG/ITB/ITB_032004.pdf, slide 47.

³⁶ *Ibid.*, slides 10, 11, 18.

³⁷ Rohan Gunaratna, *Inside Al Qaeda*, 80.

³⁸ Dan Verton, *Black Ice: The Invisible Threat of Cyber-Terrorism* (New York: McGraw-Hill/Osborne, 2003), 89.

³⁹ Ariana Eunjung Cha, “From a Virtual Shadow, Messages of Terror,” *The Washington Post*, October 2, 2004.

specialized military forces are needed to track, apprehend, and kill its fighters a few at a time. Even then, Al Qaeda's organization is so slippery that very specific and timely ("actionable") information is required to eliminate its terrorists, even one by one.

Al Qaeda is patient in collecting information, alert to opportunity, and shrewd in the timing of its strikes. What it lacks in physical capabilities it makes up with a kind of time-information advantage that depends above all on cognition. (Whether this cognition has intuitive and rational components goes beyond our research, but it seems quite plausible.) While the vulnerabilities of Al Qaeda and the forces fighting it are highly asymmetrical, its aim is to expand and use its time-information edge to survive while threatening the survival of its targets.

In line with this, Al Qaeda knows that people and information, however distorted, are its most valuable assets, and it targets its resources at the intersection of people and technology. It recruits persons with technological expertise and aptitude, who are then given internal training or sent to public schools, often for education in computer science, engineering, and electronics. "Recruitment and training for high-tech assignments (are) done very carefully, similar to how a military organization would assess both the intelligence and physical condition of volunteers for special operations units."⁴⁰

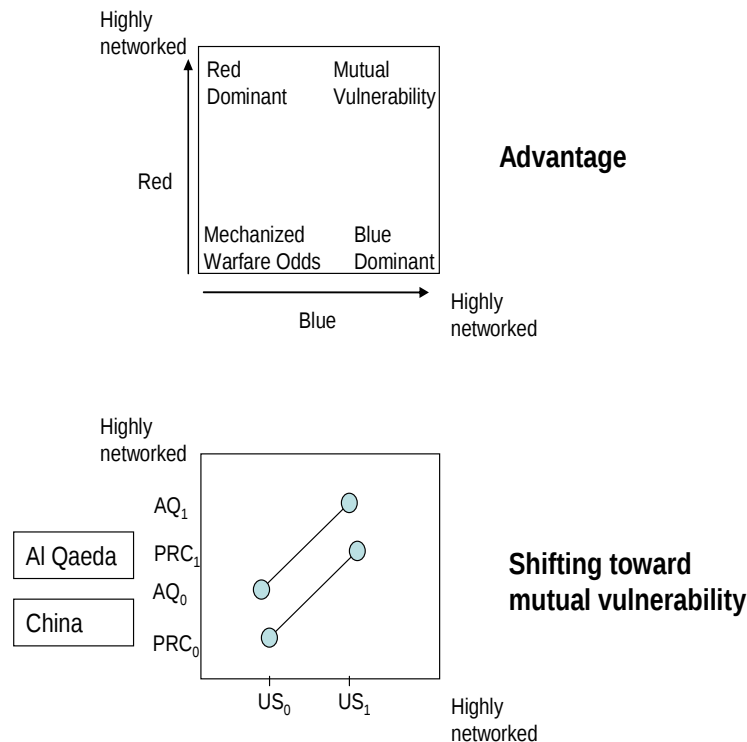
The Al Qaeda threat, while critical in its own right, spotlights a key point: the shrewdness, focus and determination with which a state or group exploits networks are as important as technical infrastructure, know-how, and organization. The key to exploiting networks is to develop and empower human beings, good or evil, to solve complex problems. In the case of adversaries, it matters less how they measure against U.S. networking concepts and capabilities than whether they are becoming harder to defeat.

Adapting to Networked Adversaries

Generally, what could be happening is depicted in figure 3. All else being equal, forces that are networked may enjoy dominance over those that are not, in the southeast or northwest quadrants. However, as adversaries (red) become more networked, moving toward the northeast, the invulnerability and thus operational dominance of U.S. forces (blue) will be eroded. This creates a degree of red-blue mutual vulnerability, even though U.S. forces will remain stronger as well as superior in their use of networking.

⁴⁰ Dan Verton, *Black Ice*, 86.

Figure 3: The Shift Toward Mutual Vulnerability



Anticipating networking by adversaries, the United States must develop warfighters with those particular cognitive abilities that offer operational advantages under conditions of mutual vulnerability. The most critical such abilities are those that turn the time-information relationship to advantage, rather than exploiting one by sacrificing the other. Four such abilities are:

- Anticipation—getting the jump on the enemy
- Decision speed—gaining time at critical moments
- Opportunism—exploiting non-linearity
- Fast adaptability—processing experience to improve performance in real time

These abilities depend on a combination of reliable intuition and efficient reasoning; one without the other will come up short.

A force with people—individuals and teams—who are endowed with these abilities and able to use them to gain time-information advantage can cause less battle-wise opposing forces to seem, in effect, more “mechanized,” pushing them back toward the corner of figure 3 where one force is vulnerable and the other is invulnerable. These abilities and the advantage that they can provide may even allow a force to engage the opposing force without being likewise engaged. Indeed, success may come in the form of prevailing without having to engage at all because the time-information-disadvantaged force—even though networked—knows it will lose.

To illustrate the importance of these cognitive abilities, imagine special-operations forces (SOF) inserted into a remote ungovernable region that has become a terrorist haven. The

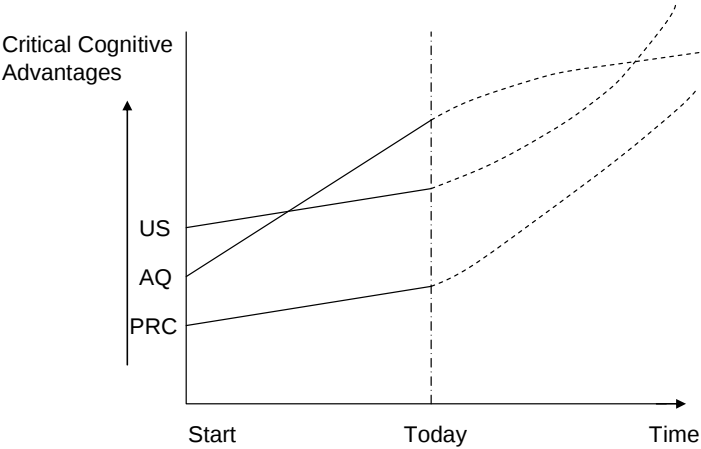
SOF are networked with precision sensor- and weapon-bearing drone aircraft and other intelligence and strike capabilities, and they have enlisted local scouts and informers. They are seasoned, disciplined and skilled fighters, and they can move quickly. The terrorists are poor in technical sensors but have better human sensors than the SOF. They are dispersed yet able to communicate with one another, though at some risk of discovery. Learning of the SOF strength, the terrorists' aim is to survive, not to fight and defeat SOF. The SOF rely heavily on experience (e.g., in Afghanistan) in which the terrorists fought then fled. Wrongly anticipating this same pattern retards SOF decisionmaking and causes a missed opportunity to cut off the terrorists' escape routes. The time it takes the SOF to analyze fresh information and adjust their plan is enough for the terrorists to melt into the wilderness, or the population, to wait and plan new terror. By cognitive failure, superior and better networked SOF lose the time-information advantage and therefore the battle.

Thus, battle-wisdom can be thought of as melding reliable intuition and efficient reasoning to gain time-information abilities and advantages in complex networked operations. The objective of building battle-wise forces, then, is to foster these abilities as a way of gaining and holding an operational edge even in conditions of mutual vulnerability. Being battle-wise does not guarantee success—it is just one of many factors in warfare in the current era. But it can tilt the odds.

Individuals are more likely to gain such critical cognitive abilities if they are able to learn in action and willing to take responsibility for the consequences of their decisions. These prized traits—to learn and to lead—are crucial in identifying, developing, and using battle-wise military decisionmakers, regardless of rank. Just as lieutenants must be willing and able to lead, lieutenant generals must be willing and able to learn.

The effectiveness of this bundle of cognitive abilities and traits depends on self-aware use of intuition and reasoning in decisionmaking and decisionmakers. Although U.S. forces will remain superior in firepower, they stand to lose critical operational advantages, with possible strategic implications, if adversaries gain a battle-wise edge. If U.S. forces do not gain and hold this edge over networked terrorists and networked Chinese forces, for example, the ability of the United States to advance its global security interests and responsibilities may suffer. As figure 4 suggests, it is not pre-ordained that the United States will win this race. In their own way, Al Qaeda and its terrorists may be learning faster than the U.S. military and its warfighters how to exploit networks. And China, while slow and well behind the United States, could improve its rate of learning.

Figure 4: Battle-wise Learning Curves



Improving Cognitive Performance in the Civilian World

Before looking at how to enhance problem-solving capabilities in the military, it is worth examining how non-military organizations are attempting to do so. For all the differences, corporations in competitive markets are facing the same basic challenge as armed forces: exploiting networks to gain advantage by improving how people sense, reason, decide, and act under pressure and in the face of complexity. In seeking “business-wise” executives and employees, companies want strong intuitive and reasoning skills, a predisposition toward learning, and a willingness to take responsibility and risk failure. They stress recruiting the brightest people they can find and then augmenting their abilities by focused training.

A study of eleven companies that have consistently outperformed the market revealed an especially high priority on hiring the right people over corporate strategy, vision, or technology. By hiring intelligent, versatile, self-aware people, a company can create a culture of objectivity, adaptability, and flexibility—all of which are needed to thrive in a complex and dynamic environment.⁴¹ While good companies seek specific knowledge and skills, their emphasis is on personal qualities and cognitive abilities.

The benefit of finding and hiring people with “the right stuff” is hardly a groundbreaking revelation, but one that may not be given enough attention by managers preoccupied with action and quarterly results. Furthermore, it is often assumed that education, training, and corporate culture will determine people’s attitudes, talents, or motivation levels. Research suggests otherwise. A survey of 80,000 managers from 400 companies found that each employee’s nature and talents are considered unique and that people don’t change their behavior that much.⁴² Like a good professional football coach drafting players based on athleticism, the best managers hire for talent and then assign and groom people for responsibilities where they can become “more of who they already are.”⁴³

Successful companies thus deem it strategically important to have people with qualities like those of the battle-wise individual. While companies rely mostly on hiring to satisfy these needs, they also use training and education, especially “self-directed learning”. At Southwest Airlines, “employees who embrace learning as a life-long pursuit are more alert, better informed, and more creative. This translates into new ways to simplify operations and cut costs, and new ways to better serve customers.”⁴⁴

⁴¹ Jim Collins, *Good to Great: why some companies make the leap— and other’s don’t* (New York: Harper Collins, 2001), 41.

⁴² Marcus Buckingham and Curt Coffman, *First, break all the rules: what the world’s greatest managers do differently* (New York: Simon and Schuster, 1999).

⁴³ *Ibid.*, 56. Gallup’s findings are based on in-depth interviews with over 80,000 managers in over 400 companies.

⁴⁴ Kevin Freiberg and Jackie Freiberg, *Nuts! Southwest Airlines’Recipe for Business and Personal Success* (Austin, TX: Bard Press, 1996), 113.

At the heart of learning is the ability to adapt to complex and dynamic situations—an art that is not stressed enough in traditional learning models. Self-directed learners take chances, are humble and reflective, eagerly collect information and views from others, and are open to new ideas and personal challenges, even at the risk of failure.

The more unstable the environment, the more important self-directed learning is. Indeed, there is a correlation between self-directed learning and strong performance in jobs that involve a high degree of change.⁴⁵ Of course, the organization must supply the tools and opportunities for employees to smart-pull the information they need to learn and to receive feedback from the decisions they make in a timely manner.⁴⁶ Self-directed learning can be more effective than organization-directed learning because it offers greater relevance to and focus on the individual's needs, flexibility in the sequence and tempo of learning, development of problem-solving skills, and lower costs.⁴⁷ Companies that promote self-directed learning, e.g., Xerox, Motorola, Honda, Corning, and General Electric, have cut cycle times for introducing new products in half, with corresponding increases in market share—a feat of time-information superiority.⁴⁸

In addition to finding and grooming people with good decisionmaking abilities, a growing number of companies, large and small, are distributing decisionmaking authority. This is now accepted as an effective way to adapt to a dynamic marketplace, when problems are too complex, fluid and unfamiliar for the corporate front office to grasp, much less solve. But, again, distributing authority is not enough—the cognitive strengths of employees, their readiness to take responsibility, and their adeptness at acting in concert are also crucial to increasing the performance of an organization as a whole.

Finally, corporate experience with collective intelligence and decisionmaking is worth noting. Cross-boundary teams can increase the quality of decisions through diverse thinking and greater inventiveness than most individuals have. One organization that effectively leverages the collective intelligence of its employees is General Electric's jet-engine plant in Durham, North Carolina. "GE/Durham" consistently produces the highest quality jet engines in the industry. Its success comes largely from cross-training, teamwork and collaborative decisionmaking. It has one manager for its 170 employees, who work in teams of 15 or so people and make decisions through dialogue and consensus.⁴⁹ Employees are trained in teams, and hiring takes into consideration an individual's collaborative attributes: supportive, communicative, flexible, tolerant, and open to others' views and new ideas. Because individuals answer to teammates, feedback is continuous. With this system, GE/Durham teams learned in a mere eight weeks to produce an engine at 12% of the cost of a more orthodox plant that had produced the engine for years.⁵⁰

⁴⁵ Ibid., 40.

⁴⁶ Paul Guglielmino and Lucy Guglielmino, "Moving Toward a Distributed Learning Model Based on Self-Managed Learning," *SAM Advanced Management Journal*, Summer 2001, 39.

⁴⁷ Ibid., 39.

⁴⁸ Ibid., 36.

⁴⁹ Charles Fishman, "Engines of Democracy," *Fast Company*, Issue 28, October 1999, 174.

⁵⁰ Ibid., 174.

What we take from these and many other examples is not simply that companies are getting flatter, decentralizing authority, and fostering collaborative forms of decisionmaking—that has been known since such ideas came into vogue years ago—but that they are on average producing superior results by doing so. We find as well that investment and trust in people to make good judgments and solve complex problems is deemed a key to competitiveness in high-tempo, high-pressure markets. Just as we see that incorporation of information technology is now yielding brisk productivity gains, we see that efforts to expand, invigorate, connect, and focus cognitive powers is bearing fruit.

Where corporations and the armed forces differ in trying to improve cognitive capability is in how to get the right people in the first place. It is not hard for corporations to spot potential for future top performance, and when they do, the strong ones have the financial wherewithal and flexibility to recruit aggressively. For instance, as a matter of corporate strategy, Google identifies the best search-engine people available and manages to hire about 90% of them.⁵¹ It is far harder to recognize battle-wise potential in military recruits, and the armed forces cannot afford to do what Google does.

⁵¹ Keith H. Hammonds, “How Google Grows...and Grows...and Grows,” *Fast Company*, Issue 69, April 2003, 74.

Building a Battle-Wise Military

For the armed forces, a battle-wise lead can be gained and kept by: (a) improving the cognitive abilities of individual warfighters; (b) reforming command and control to harness these abilities; and (c) enhancing the collective cognitive power of teams.

- Battle-wise individuals can be developed by strengthening recruiting standards and strategies; investing more in early, demanding and relevant education and training; and identifying, retaining, promoting, and utilizing those who excel.
- Command and control reform should encompass expanding the opportunity for battle-wise problem solving from “the few” senior officers to “the many” junior ones; permitting more effective horizontal collaboration; and enabling warfighters, units and whole forces to solve problems at the lowest appropriate level.
- Collective intelligence can be achieved by forming coherent, if temporary, teams to tackle particular operational problems, thus delivering sounder decisions and offering greater flexibility than vertical command and control.

These three efforts must go hand-in-hand. It will take more battle-wise warfighters to justify wider distribution of decision authority; it will take both more battle-wise warfighters and distributed authority to enable ad-hoc teams to tackle complex and urgent operational problems; and progress in team problem solving will repay and motivate both more investment in developing battle-wise people and reform of command and control. Therefore, although efforts toward these ends will involve sundry measures in disparate areas and organizations, from personnel policy to joint command structures to cultural change, it is important to pursue them within a purposeful, coherent strategy.

Developing the Individual

The U.S. military is justifiably proud of the abilities and attitudes of its uniformed men and women since the advent of the all-volunteer force following the Vietnam War. Recruitment and retention of high-quality people—hallmarks of this success story—have held up well, despite heightened deployment frequency and hostile duty since the end of the Cold War. Even with the information and geo-political revolutions, we have no reason to think that the *general* intelligence, however defined, of those entering or serving in the military falls short of the *general* demands of operations.

Nonetheless, there is room to examine how and how well the U.S. armed forces select and prepare people to solve problems in combat characterized by unfamiliar circumstances and abundant data. It is fair to ask whether current personnel systems should be adjusted to favor the decisionmaking attributes that seem especially important for networked warfighters opposed by networked foes, i.e., anticipation, decision speed, opportunism, rapid adaptation, willingness to take personal responsibility, and the capacity for self-directed learning. And it is worth considering whether training and education of warfighters should be geared more toward decisionmaking methods that integrate intuition and reasoning to gain time-information advantage.

DOD has several levers to strengthen battle-wise abilities and methods: recruitment, selection and assignment, education and training, evaluation and reward, and career management and retention. In regard to recruiting, it would be ideal if an exact battle-wise profile could be used to find, filter, and attract the right people. However, it is hard to judge early on who will perform well in battle. In fact, the surest indicator of effective future performance in combat is previous performance under similar conditions.⁵² Moreover, the methods currently used to assess recruits for the U.S. military are very general. For enlisted personnel, it is something called the Armed Forces Qualification Test (AFQT), which purports to predict “productivity.” For officers, admission to a service academy or reserve-officer program anticipates warfighting cognitive demands barely, if at all. While such processes can screen out individuals who are clearly not suited for combat, they are blunt instruments that cannot identify people of high battle-wise potential.

Nevertheless, there are ways that the military could improve its intake of persons with desired operational-cognition qualities. The first is to hire people with some relevant problem-solving experience. Unlike corporations, the military does not have the option of lateral entry in its current personnel system. The traditional argument against lateral entry is that entrants would not be able to function well in the military without going through every stage of military-specific training and experience, starting at the beginning and the bottom. Indeed, some aspects of military training and experience, especially combat, are unique. However, with the problem-solving demands on military personnel increasing, analogous private-sector experience might provide some of the raw talents and experiences that the military needs: analysis-under-pressure, learning-in-action, making sense out of large volumes of information, and making decisions in the face of complexity, uncertainty, and risk of failure. DOD could bring in such people above entry level and then furnish them with specific warfighting training.

While it may fly in the face of tradition, it does not fly in the face of reason that, to take an obvious example, a superb law-enforcement officer could, with intensive training, become a mid-level battle-wise officer. Of course, there are potentially serious implications for fairness, morale and cohesion associated with lateral-entry recruiting. Moreover, the higher the military rank the greater the need for institutional knowledge—“firm-specific knowledge,” in the argot of economics—that cannot be acquired anywhere else. Finally, coaxing an able person from another profession into the military would likely require significant financial incentives to compensate for career and corporal risks. Still, some experimentation may be indicated.

At most, lateral entry could account for just a small fraction of total recruits. The military must bring in most people at the bottom of the pyramid. Therefore, another method that should be studied is to identify those recruits with high battle-wise potential as early as possible through such sorting mechanisms as basic training and observation, and then

⁵² James R. Hosek, “The Soldier of the 21st Century,” in *New Challenges, New Tools for Defense Decisionmaking*, Stuart E. Johnson, Martin C. Libicki, and Gregory F. Treverton (eds.), (Santa Monica, CA: RAND, 2003).

place them on a career path that maximizes their development in this direction. Of course, doing this effectively would require developing a profile against which to assess and track cognitive capacity for warfighting.

However people with battle-wise potential are identified, the military will need to compete for them with the private sector, which will be looking for similar qualities for a similar reason, namely, to exploit abundant information in dynamic and confusing conditions. It would be prohibitively costly for the military to match such remunerative fields as business, medicine, and law by raising pay across the board. But recruitment, as well as subsequent retention, of battle-wise talent could be improved by increasing the steepness at which pay grows in relation to rank—now quite flat by industry standards. In addition, offering valuable education and training can help attract high-quality people, who are sophisticated enough to weigh long-term earning power, not just pay in the first few years. Of particular value in recruiting is education and training that are relevant whether the individual stays in or leaves the military, which is the case for schools and courses that teach skills and ways to solve complex problems.

Still, the military cannot count on recruiting and early sorting alone to produce battle-wise warfighters, given the difficulty of measuring potential and the costs of out-bidding industry for people with ideal aptitudes. So it must invest heavily in preparing promising people to meet the mental demands of warfighting. Education and training are thus important not only to recruit and retain but also to develop battle-wise capacity and performance among the troops. They must begin early, be competitive, and provide for failure.

U.S. military education and training are as good as any in the world. If they are lacking, however, it may be in short-changing analytic skills. Those who have taught in and studied in the U.S. professional military education system know that there is more emphasis on facts than analysis—on what one knows rather than how one thinks. In a turbulent world, with abundant information, the latter is paramount.

The requirement to train soldiers for traditional military functions is not going to disappear anytime soon. However, future warfare will demand unprecedented levels of initiative, decision speed, adaptability, opportunism, and cross-boundary collaboration. “The future will require that more of our people do new and much more complicated cognitive tasks more rapidly and for longer continuous periods than ever before...this amounts to a qualitative change in the demands of our people that can not be supported by traditional kinds of training.”⁵³ Training is designed to teach soldiers new skills, but it can also give them experience with combat-like situations. The more circumstances one has experienced realistically in training, the more patterns one will be able to recognize, even in unfamiliar situations. If, as a result, intuition can be applied across a wider range of contingencies, it can help tighten reasoning, eliminate unsound options, and substitute for reasoning when relevant data is scarce.

⁵³ Defense Science Board Task Force on Training for Future Conflicts, *Final Report*, June 2003, available at <http://www.acq.osd.mil/dsb/reports/tfc.pdf>.

One way to improve the intuitive aspect of decisionmaking is to isolate the types of decisions needed in a variety of contingencies, even if the contingencies themselves are unforeseeable and prove unfamiliar. Trainees must then practice those decisions repeatedly, review the consequences, and make appropriate adjustments next time around.⁵⁴ This method is currently used by the U.S. Army's National Training Center.⁵⁵ Simulation is especially promising. One of the most promising systems under development is called the Joint Fires and Effects Trainer System.⁵⁶ With it, soldiers can train in a wide variety of operational environments in an extremely short period of time. The simulations are less expensive and more compressed than real-life exercises, and they can be changed in a day to reflect up-to-the minute intelligence on threats and theaters of concern. This can improve a soldier's intuition by increasing the number of combat situations he or she experiences in a given time period.

However the U.S. military endeavors to develop more battle-wise soldiers, measurement of the efficacy of training methods has never been more critical. "Training's achievements, its failures, and its costs are not routinely visible to those with authority over discretionary funding."⁵⁷ To accomplish this, the performance of forces undergoing training must be assessed at the individual, unit, and system-wide levels. One way to do this is to require the military to deliver an annual training report card directly to the Secretary of Defense.⁵⁸ The use of standards and metrics emphasizing the growth of battle-wise abilities could be part of such a process.

If the military succeeds in growing more battle-wise soldiers, it will then face the challenge of keeping them. The core cognitive strengths that define such people are in high demand in the private sector. Unfortunately for the military, the business world offers higher pay, more flexible careers, and more stable—if less exciting—lives than the military, especially to the most able individuals. Even now, many high-performing soldiers leave before the military realizes a positive return on investment in the education and training it has provided them. This problem could be aggravated if the military invests even more, and earlier, in people with high cognitive potential.

The flip side of this problem is that the existing personnel system makes it difficult to discharge people it does not need. The effect of these two factors is that the military has a sub-optimal mix of soldiers. "On average between 1999 and 2002, the services had shortages in about 30 percent of their occupations, while they were overstaffed in 40 percent."⁵⁹ One way to deal with this problem is for the military to conduct rigorous sorting before the 10-year mark. However, because the current pension system does not provide for vesting until 20 years of service, soldiers who stay in past 10 years tend to

⁵⁴ Ibid., 28. See Gary Klein, *Intuition at Work* for a detailed training methodology. Klein has developed training programs that have been adopted in varying degrees by the armed forces, fire departments, and the National Fire Academy.

⁵⁵ Richard Pascale, "Fight. Learn. L*E*A*D," *Fast Company*, August/September 1996, 65.

⁵⁶ Steve Silberman, "The War Room," *Wired*, September 2004, 151-155, 171-173.

⁵⁷ Defense Science Board, *Final Report*, 7.

⁵⁸ Ibid., 70.

⁵⁹ Cindy Williams (ed.), *Filling the Ranks: Transforming the U.S. Military Personnel System*, BCSIA Studies in International Security, (Cambridge, MA: MIT Press), 2.

want to stay for 20. Moreover, it is hard to justify releasing unvested soldiers after 10 years based on performance. By sorting rigorously before soldiers reach the 10-year mark, the military can target those soldiers who will provide value in the long run and focus on retaining them as long as possible.⁶⁰ In addition, the military could better shape its talent to meet its warfighting needs with a more flexible retirement system, including vesting by 10 years and offering thrift-savings programs.⁶¹

In addition to helping with recruitment and operational performance, valued education and training can aid retention, up to a point. True, the better job DOD does in creating battle-wise people, the harder it may be to hang on to them. On the other hand, there is evidence that if an organization gives people marketable skills, they will actually stay in longer than if they do not receive such skills: “There is a strong correlation of psychological commitment and intent to stay (loyalty) with an organization’s efforts to make an individual more marketable; the risk of losing employees is greatly increased when organizations fail to provide such opportunities.”⁶²

Still, the recruiting, sorting, and development strategies suggested here, along with greater emphasis on widely valued cognitive abilities, would potentially make it difficult to keep battle-wise warfighters beyond 10 years or so. These people will have received exceptional education and training early and, by vesting at 10 years, will have less incentive to stay for 20. However, this may not be a problem in the new era. Networks can flatten organizations, including military ones, by decentralizing authority, eliminating management layers, and increasing spans of control. Consequently, military career pyramids, like those in other professions, could become flatter. All else being equal, this will reduce quantitative long-term retention requirements. Moreover, with decisionmaking authority being distributed outward and downward, junior people will be asked to add more value in operations. Simply stated, if it now takes a colonel with twenty years of service to solve certain types of problems, in the future such problems may be handled by a major with ten years of service. If it succeeds in creating battle-wise soldiers early enough, the military may not need to retain them for 20 years to recoup its investment.

In sum, in light of the importance of finding and developing people with battle-wise abilities, the military might consider some lateral-entry hiring, steeper pay increases with promotion, early sorting, and a more flexible retirement system. Education and training geared to sharpening cognitive skills could help in recruitment, sorting, operational performance, and, to some extent, retention. If, however, a strategy of investing heavily and early in development of battle-wise warfighters means that many of them will leave for more lucrative—not to say safer—professions, this may be tolerable in view of the delegation of authority and flattening of military hierarchies.

⁶⁰ Yet another problem with the current personnel system is that the military often loses the people it most wants to keep at the 20-year point. After they have vested in their retirement system, many soldiers leave the military to begin second years in the private sector.

⁶¹ See Thomas M. Strawn, “The War for Talent in the Private Sector,” *Filling the Ranks*, 88.

⁶² *Ibid.*, 89.

Reforming Command and Control

A network can be thought of as a mobilizer of many problem-solvers, each contributing to the cognitive and thus the operational effectiveness of the whole organization. If the problem-solving abilities of each networked warfighter can be improved by the sorts of measures suggested in the preceding section, then it makes sense to engage many of them (up to a point) in decisionmaking and to increase the demands on each. For this reason, we say amen to calls for more decentralized military command and control.⁶³

Decentralized command and control runs against the grain of military culture, in which decisionmaking authority tends to drop off steeply the further down the hierarchy and the farther away from headquarters one goes. In the traditional perspective, this pattern reflects less a hoarding of authority than a natural distribution of responsibility from the strategic to the operational to the tactical planes as one moves down the hierarchy. However, that three-plane model has been disturbed by the growing speed, fluidity, and ambiguity of warfare, which blur and compress these planes, increase the significance of tactical decisions, and reward horizontal, peer-to-peer, collaboration. Moreover, the traditional view of decisionmaking presumed that the commander at the top would possess more relevant information than the warfighter on the edge, which may no longer be valid for many situations. The beliefs of the old culture—that experience counts above all and that top commanders are better informed than lower ones—are getting battered by the geo-political and network revolutions mentioned earlier. In unfamiliar conditions and with data easily shared, mobilizing the battle-wise many is both needed and possible.

In most enterprises, especially information-rich ones, it is more productive to let people use and test the limits of their talents within broad guidance and boundaries than to rely on rigid job descriptions and a regime of strict dos and don'ts. The gains in creativity and output from informing, freeing, and trusting people outweigh the risks averted by constricting and directing them. Networks ought to give every decisionmaker the ability readily to pull all available and relevant information. And command and control ought to help warfighters use that information to make battle-wise decisions.

The specific cognitive abilities that are, in our view, crucial to operational success—anticipation, reaction speed, opportunism, and rapid adaptation—all strongly correlate with decentralization of authority from top to bottom (or edge). Precisely because combat success increasingly depends on turning the time-information relationship to advantage, the case for decentralization is a strategic one.

Decentralization must, of course, go hand in hand with having more battle-wise warfighters throughout the force, up and down the ranks. Entrusting junior officers or non-commissioned officers in the field to make quick, critical, and sound judgments demands that they can intuit reliably and reason efficiently, are aware of their analytical and experiential strengths and limitations, can learn in action, and are adept at the sort of battle-wise decisionmaking described earlier. Therefore, decentralization of decision

⁶³ David S. Alberts and Richard E. Hayes, *Power to the Edge*.

authority to take advantage of networking will both require and reward efforts by the armed services to build up these cognitive strengths.

At the same time, the generals and admirals at the top of a force must focus on what *they* are uniquely placed to decide, e.g., strategic direction and choices with strategic implications. There is anecdotal evidence from exercises and live combat that the improvement of information systems and displays is leading to greater, not less, micro-management. The danger of micro-management is aggravated by the fact that, in the U.S. military, joint organization for operations exists only at the top—namely, the joint task force command and, in a partial way, component commanders.⁶⁴ As networks permit deeper operational integration, the lack of joint command and control below this level will hamper performance and impel senior joint commanders to exert more, not less, micro-management—the opposite of what is needed and possible.

Extending decisionmaking to more warfighters on the network depends on devising command-and-control architectures to permit the shifting of authority downward and outward. But reform is not just about decentralization, because networks not only inform warfighters but also make them interdependent and expand options for collaboration. Command and control architectures should accommodate the need for units and decisionmakers throughout the networked force to support and be supported by others, regardless of geography, service boundaries, and normal operational command boundaries. Permitting local and peer-to-peer problem solving may weaken vertical control, but it also demands strong and open horizontal and diagonal links, which do not easily fit with rank, structure, and formal command and control. Even as top commanders delegate their traditional authority, they are indispensable in managing and mediating interdependencies and in allocating scarce resources.

In the transition from control by the few to empowerment of the many, it may be useful to have a few enduring rules governing who should make what decisions:

- First, commanders should communicate the envelope within which subordinates may and should operate, defined by objectives, limits, and available resources. The limits of authority should be predicated on whether decisions (including bad ones) taken by subordinates may have consequences (including unintended ones) outside their space.
- A second rule might be that the decisionmaking authority of an individual is contingent on that individual's having at least as much information as a superior commander does. Even in a networked environment, it will often be the case that headquarters has some information bearing on a tactical situation that cannot be rapidly shared with the warfighter, perhaps for security reasons.
- Third, any individual who does not feel equipped with the intuitive and reasoning powers to make a sound decision should unhesitatingly seek and receive guidance. Self-awareness of one's limitations is a strength, not a weakness.

⁶⁴ Since joint component commanders are in essence service commanders with joint operational responsibilities, it remains to be seen whether they represent a bridge to a future of more extensive joint command and control or instead a blockage to that future—an issue outside the scope of this study.

To illustrate, let's revisit the major leading the ambushed column in the African peacekeeping operation. If he decides wrongly and fails in his mission or suffers high casualties, but his decision does not have significant consequences outside his envelope of responsibilities, then giving him decision authority was probably the correct move. However, if his misjudgment exposes other units to a larger losing battle or jeopardizes the peace of the province, perhaps the decision should not have been left to him to make. Similarly, if the major's superior knows but cannot communicate, for whatever reason, that the window to carry out this unit's mission is closing, the superior may have to tell the major that pulling back is not an option. Finally, if he or his superiors are convinced that the situation is more complex and dangerous than he is prepared for, it might be best not to risk failure, even within his envelope of responsibility.

Intangible qualities—self-awareness, trust, and a flexible feel (not some rigid structure) for who is best placed to decide what—are increasingly important in command and control. They both rely on and can reinforce battle-wise individuals. Other than combat itself, there is nothing as effective as exercises to inculcate forces with them.

Developing Intelligent Teams

Network theory, more or less confirmed by practice, suggests that ad-hoc teams will self-organize to deal with common problems, enabling an organization to continuously optimize its resources despite uncertainty and change. This raises the question of whether and how teams can be battle-wise.

In a fascinating recent book, *The Wisdom of Crowds*, James Surowiecki shows that groups consistently produce solutions and decisions superior to those produced by all but the brightest of the individuals in the group—now and then even better than the brightest. The best way to guess the number of jellybeans in a jar is to ask a large number of people and then take the average. The best way to set odds on a football game is to leave it to a large population of independent bettors. The fairest way to decide the fate of an accused is, usually, by jury. The reason for this, simply put, is that the errors of individuals tend to cancel out one another as numbers increase, leaving the average to be that much more on the mark. Such collective wisdom only works if there is ample diversity and independence of views among the participants, be they jellybean counters, gamblers, or jurors. That way, the full range of experiences, perspectives, and information of the many are in play, resulting in a better answer than if based on the experience, perspectives, and information of a few. Absent substantial diversity and independence, “groupthink”—the assassin of reason—may rear its head.

We resist the temptation to apply the crowd-wisdom principle wholesale to military problem solving. After all, the warfighters of a force are not all faced with the same tactical problem but myriad ones. However, this approach could have merit in the case of a group of people organized to face a common problem, which is the very idea of ad-hoc, cross-boundary, military-operational teams. Assuming they are accommodated by flexible formal command and control, such teams can bring to bear diverse perspectives on common problems—precisely the conditions in which collective wisdom excels. Thus,

crowd-wisdom could translate into battle-wisdom not at the wholesale (i.e., force) level but at the retail (team) level.

For our purposes, the most relevant issues are whether collective wisdom and its sibling, collaborative problem solving, are conducive to the particular cognitive abilities that are especially important in the networked warfare and messy contingencies of the new security era, and, if so, what can be done to foster these abilities.⁶⁵

While evidence suggests that collaboration is usually better than solo problem solving, it may not be that simple. There is a time-information trade-off between the cognitive speed, agility, surprise, and adaptability that comes from singular decisionmaking and the quality of decisions informed by the views of members of a team. So, as we consider whether collective or individual problem solving is best when trying to maximize anticipation, reaction speed, opportunism, and fast adaptation, the answer surely is: it depends. Take the case of the major and the ambushed unit mentioned earlier. All else being equal, forming a team with other, networked unit commanders for the sake of deciding whether to get his unit out of harm's way or instead to engage in a fire-fight would offer little gain in the quality of the decision and significant risk to its timeliness. Yet, once ground and gun-ship support arrives, it may make more sense for the several officers concerned to discuss and even decide together whether to eliminate the ambushers or instead brush them aside and get on with the mission.

If ad-hoc teams can be “crowd-wise,” there is still the question of how to make them battle-wise. A reasonable starting point could be the same recipe that appears important for the individual warfighter: a provisional decisionmaking approach to gain time and information, self-awareness of collective experiential and analytical limits, the ability to learn in action, and an emphasis on the abilities that create operational time-information advantages—anticipation, rapid decisionmaking, opportunism, and rapid adaptation.

This is a tall enough order for individuals; achieving it for teams, however promising in theory, will be very hard. Such collaboration can be tested and strengthened by exercises and other training. But since the actual forces on any given operational network or mission are fluid and dependent on circumstances, it is not clear how to choose the assortment of units to be exercised. Obviously, more cross-service training is warranted. However, it will take considerable resources and organizational innovation to plan exercise scenarios involving various combinations of, for example, special operations forces, bomber squadrons, unmanned airborne sensors, land-forces, missile-carrying submarines, and aircraft carriers. And it will not be easy to build trust and appreciation of how teammates approach problems if the teams form only after a threat or opportunity appears. The concept of collective wisdom in military operations—creating as well as using it—requires much more thought, research, and experimentation.

⁶⁵ A third relevant issue is how to harmonize team problem solving with vertical command and control. This requires and is getting analytical attention both in and out of DOD, and we will not tackle it here.

Suggestions

If the U.S. military is to exploit its network advantage to preserve its operational and strategic advantages, it will have to consider a variety of policies and measures aimed at developing (a) more battle-wise warfighters, (b) command and control systems that allow, support, and exploit more battle-wise warfighters, (c) battle-wise self-forming teams, and (d) decisionmaking that integrates intuition and reasoning. Those we flag below are by no means an exhaustive list:

1. *Recruit people with exceptional battle-wise aptitude.* To the extent possible, refine and use battle-wise qualities in recruitment of at least some incoming people. Use steeper pay tables and the promise of highly valued education and training to attract people with these qualities.
2. *Educate and train early, competitively, and well.* Stress early enhancement of key cognitive and adaptive decisionmaking skills in schools that recognize true excellence and permit failure. Foster self-directed learning.
3. *Sort and select as education, training, and operational experience permit.* Because it is difficult to recognize battle-wise potential among recruitment candidates, filter internally for further development and assignment of warfighters. Intensify sorting as the 10-year mark approaches.
4. *Rethink retention in light of battle-wise needs and flatter organization.* Gradually shift emphasis from quantities to observed battle-wise qualities in retention. Use career-long education and steeper pay tables to retain the best for full careers. Make the retirement system more flexible.
5. *Accelerate command and control research and reform.* Intensify experimentation with decentralized joint command-and-control networks, peer-to-peer collaboration, ad-hoc teaming, and the three in combination.
6. *Foster collective intelligence.* Train and exercise self-organizing teams as a way of increasing the collective battle-wisdom that can be brought to bear on operational problems.
7. *Conduct further research and analysis.* Pursue the issues raised by this and other papers on whether and how to improve cognitive effectiveness.
 - What are the prerequisites adversaries must meet to be able to exploit networking militarily, and how might they meet them?
 - If and as adversaries are able to exploit networking, what will be the effects on U.S. force vulnerability and performance?
 - What are the strategic and security implications of these operational effects?
 - What are the most important cognitive abilities of warfighters in the new (and ever-changing) security, operational, and information environment?
 - What profile of warfighting cognitive aptitude and qualities should be reflected in recruiting standards and strategies?
 - Should quantitative and qualitative retention goals change with the advent of networking, the decentralization of authority, the

flattening of organizations, and the stress on people with key cognitive abilities?

- Do professional military education systems place sufficient emphasis on developing and recognizing these abilities and the decisionmaking methods that utilize them to best effect?
- How should training and exercising be sharpened to make intuition more reliable and reasoning more time-efficient in operational problem solving?
- How should command and control networks, structures, and procedures be designed and developed to improve the distribution of authority and the efficacy of peer-to-peer collaboration?
- How can networks enable teams to think and decide without sacrificing timeliness?
- How can the goal of and progress toward improved cognitive performance in networked operations be measured and monitored?
- Who should do what to make progress?

Conclusion

Because the goal described in this essay—exceptional minds making sound decisions in the heat of battle—has *strategic* significance, we conclude at that level.

Every so often, the focus of military competition shifts. By the late 19th Century, grand fleets and continental armies had become less important as industrialized military power moved to the fore. Germany, Great Britain, the United States, and Japan stood apart and competed fiercely—and violently—because of their ability to combine industrial and military excellence. In the aftermath of World War II, nuclear and aerospace power eclipsed mechanical power. Only the two superpowers could assemble the massive resources and expertise needed to compete in these demanding realms. By the end of the Cold War, information technology had entered the military domain. One of the superpowers—the one with no commercial markets or market-driven technologies—could not compete or keep its empire intact. With each shift, the field of competitors narrowed as fewer and fewer could marshal the requisite economic and technological resources for military purposes.

At the beginning of the 21st Century, the networking of forces promises a potent combination of awareness, precision, speed, dispersion, and integration in military operations. With its excellence in information technology, networking, and advanced military systems, the United States is and will remain the leader. Head-to-head competition with the United States is out of the question. Yet, paradoxically, the scope for military competition has been reopened by this development. Information-network technologies tend to be inclusive, not exclusive. With widely available information services, readily accessible global network infrastructure, abundant band-width, and easily acquired technical know-how, growing numbers of states and non-state groups, some unfriendly, will be able to use information networks to improve *their* operational awareness, precision, speed, dispersion, and integration.

Although enemy forces will not be able to rival U.S. military network capabilities, if they are shrewder and quicker than U.S. forces in exploiting information, the costs of U.S. military action could be increased and the certainty of decisive success could be reduced. Whether the concern is with Al Qaeda in the near term, China in the long term, or eventually some other wily and determined adversary, it is imperative that the United States sharpen the cognitive abilities and decisionmaking methods of its military personnel—battle-wise individuals and teams alike. The military needs to increase the number of minds in its ranks that have the ability to lead and make decisions under the pressures of war with the increasing complexities of a networked environment. With its exceptional people, proven personnel systems, and excellent military education institutions, the United States has all the ingredients it needs to develop forces that can not only out-fight opponents but also out-think them.