Caught in the Net: Lessons from the Financial Crisis for a Networked Future

GAUTAM MUKUNDA and WILLIAM J. TROY

Since 2000 the Department of Defense (DOD) has committed itself to implementing a vision of the future of combat usually referred to as Network-Centric Warfare (NCW). This vision, as described by the Office of the Assistant Secretary of Defense for Networks and Information Integration, holds that robustly networking the force will improve information sharing, collaboration, and shared situational awareness.[1] The DOD has invested considerable resources in its efforts to develop and implement NCW despite criticism from within and outside the armed forces.

Much of the inspiration for NCW came from the business world, particularly the technological and organizational changes associated with information technology. These business roots have been a source of ammunition for NCW's critics, who argue that, at least when it comes to operations, "uncertainty in war makes business and war incompatible . . . ." Business and war certainly have significant differences, but this critique is simply incorrect. Uncertainty is a major factor faced by businesses and militaries alike. Both compete with rivals to survive, innovate to improve their performance, and act despite uncertainty, risk, and information scarcity. These similarities are pronounced enough that, when they are correctly adopted, ideas and theories from the business world can provide insight on many issues facing militaries, including operational and strategic ones.[2]

The fact that business ideas can help militaries, however, does not necessarily strengthen the argument for NCW. The current financial crisis was caused in part by pervasive mistakes and misjudgments in the financial world. These mistakes were enabled, and their consequences aggravated, by network effects and cognitive errors rooted in technologi-

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2009		**00-00-2009 to 00-00-2009**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Caught in the Net: Lessons from the Financial Crisis for A Networked Future	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) **Parameters Army Magazine, , , ,**	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
The authors would like to thank Vice Admiral Nancy Brown, Joint Staff J-6; Lieutenant Colonel Charles J. McLaughlin IV; Colonel John P. Sullivan; Austin Long; Daniel Summers-Minette; and David Warsh for their comments. The National Science Foundation provided partial funding to Mr. Mukunda for this research. Parameters (Army Magazine), Summer 2009.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Public Release**	**14**	

cal approaches to dealing with complexity and uncertainty. Just as examples from the business world inspired NCW, the current crisis, which has a size and severity exceeding that of any since the Great Depression, illustrates risks that the designers and users of the future network have to understand and mitigate, risks not previously identified by critics of NCW. The crisis shows that while networks can substantially improve organizations' efficiency and performance, they can also leave them vulnerable to an unpredictable cascade of failures. The network-centric approach promises to allow commanders to understand battlefields with unprecedented clarity and fidelity. The financial crisis, however, shows that these tools can mislead as well as illuminate due to their simplification of a far-more complicated underlying reality. Finally, NCW will create the potential for simulations of future battlefields that would provide commanders with tools of unprecedented power for managing risk and uncertainty. Failures in risk-management models played a key role in the financial crisis, however. They can lead to massive and unanticipated errors if the models do not accurately capture reality and instead give users a false confidence in their understanding of the environment.

This article uses the financial crisis to illuminate these three potential dangers inherent in the NCW approach. This critique is not meant to suggest abandoning NCW, but rather to recommend a cautious approach to the critical endeavor of preparing the American military for its networked future, one that takes all potential risks into account.

Net-Centric Warfare Background

The movement toward NCW is official DOD policy. The last *Quadrennial Defense Review Report* in 2006 described the net-centric vision:

> Harnessing the power of information connectivity defines net-centricity. By enabling critical relationships between organizations and people, the Department is able to accelerate the speed of business processes, operational decisionmaking, and subsequent actions. Recent operational experiences in

Gautam Mukunda is a Ph.D. candidate in political science at the Massachusetts Institute of Technology. His research focuses on the role of leaders in organizational performance, military innovation, and the implications of emerging technologies.

Major General William J. Troy is Vice Director, J-8, Force Structure, Resources and Assessment Directorate, The Joint Staff. He is a graduate of the US Military Academy, British Staff College, Naval Postgraduate School, and Naval War College. He has deployed to Operations Desert Shield and Desert Storm and served as Chief of Staff, Multi-National Command-Iraq.

> Afghanistan and Iraq have demonstrated the value of net-centric operations. Ground forces were able to reach back to remote [Unmanned Aerial Vehicle (UAV)] pilots in Nevada to direct UAVs in support of their operations, achieving a level of air-ground integration that was difficult to imagine just a decade ago. Such connectivity is helping joint forces gain greater situational awareness to attack the enemy. Achieving the full potential of net-centricity requires viewing information as an enterprise asset to be shared and as a weapon system to be protected.[3]

The need for the network and the benefits it offers have a prominent place in joint and service doctrines and guiding documents. The April 2005 *Net-Centric Environment Joint Functional Concept* "identif[ies] the principles, capabilities, and attributes required for the Joint Force to function in a fully connected framework." The net-centric environment is meant to enable:

> the exploitation of the human and technical networking of all elements of an appropriately trained joint force by fully integrating collective capabilities, awareness, knowledge, experience, and superior decisionmaking to achieve a high level of agility and effectiveness in dispersed, decentralized, dynamic, and uncertain environments.[4]

This network is currently being built, piece by piece, process by process. Within the requirements process, for example, the Net-Centric Functional Capability Board evaluates future systems on their potential for incorporation into the network. Similarly, within the acquisition system there are rigorous tests and certifications that ensure new weapons and other combat systems will be compatible with the network. The Defense Department has spent, and continues to spend, billions of dollars to create a network-centric force.

This vision has generated a vigorous critical response. A starting point for critical analysis has been findings that technological superiority played a far smaller role in American success during the first Iraq War than is commonly believed. Some critics of NCW have argued that the net-centric vision, while possibly appropriate for naval and aerial combat, which are unhindered by the complexities imposed by population and terrain, is unsuited to the vagaries of land warfare. Army Colonel H. R. McMaster, for example, has argued that expectations of information dominance distract from the perpetual verities of combat by presenting the false image of a transparent battlefield. Others have focused on the apparent impossibility of gathering and analyzing the volume of information necessary to make NCW possible, or argued that the network may create problems with information security and offers capabilities ill-suited to the requirements of future wars.[5] Although these critiques have been wide-ranging and influen-

tial, there are other potential problems, three of which have been paralleled by the current financial crisis. These problems need to be mitigated by the designers and users of the network before it is implemented.

Things Fall Apart

The Duke of Wellington described "[t]he whole art of war [as] getting at what is on the other side of the hill, or, in other words, in deciding what we do not know from what we do." Even for Wellington such deductions were inherently uncertain, and it is this uncertainty that makes war as much art as science, with success dependent on the commander's "intuition and genius."[6] War is, and always has been, an exercise in decision-making under conditions of uncertainty. Modern military platforms (such as aircraft, ships, or tanks) and military formations (from infantry companies to carrier strike groups) seek to mitigate the effects of this uncertainty by, among other approaches, using redundancy and generalization. They guard against unanticipated events by devoting resources to back-ups, contingencies, and self-protection. The fog and friction of war push today's force, as they pushed all of its predecessors, toward generalization. The force deals with the unexpected, so its individual components retain the ability to succeed at a variety of tasks, rather than focusing on performing a single mission with the highest degree of effectiveness. Today's military specializes to a degree but has to compromise and retain broader capabilities due to uncertainty. These compromises are inherently inefficient. Yet today there is no other choice, because seeing the other side of a hill, and coordinating to deal with the enemy there, remain imperfect at best.

NCW's most enthusiastic proponents, however, envision a future military comprised of much more specialized units connected by the network. The network will help produce "information dominance" through its ability to rapidly combine data received by many different nodes into a coherent picture of the battlefield. American forces then can be "smaller, lighter, [and] more efficient" because they are made up of specialized units that cooperate to produce effects that previously required much larger forces.[7]

A force made up of such specialized units would be smaller and lighter, and faster and more agile. Instead of combining mass these units would combine their effects and even "self-synchronize"—work together without direction from higher authority.[8] Specialized units have advantages if the network truly allows them to cooperate seamlessly, but each single unit has less cross-functional ability and less reserve capacity to deal with unanticipated contingencies. Specialized units do one thing and do it well. If they encounter a task they cannot accomplish, they use the net-

work to hand it off or get support. Given the same amount of resources, a specialist will always outperform a generalist at the task on which the specialist is focused. The network would provide a clear enough view of the battlefield that these specialized units could reliably be in the right place at the right time. An army made up of tightly networked groups of specialized units should thus be able to outperform a traditionally organized one given the same resources.

The idea that networked specialists can outperform generalists is not a product of the information age. It goes back, in fact, to Adam Smith's description of a pin factory in *On the Wealth of Nations*. Smith described how the workers at a pin factory produce thousands of times as many pins as the same number of people would if they worked individually. This productivity is possible because each employee specializes in one step of the process.[9] The employees in Smith's pin factory were networked by their communication inside the factory. Information technology simply allows networks to diffuse across the globe.

Sophisticated modern networks, linked by computer systems and flows of trade goods, have resulted in an enormous increase in world productivity, much of it derived from firms' greater ability to specialize in a global market. This is the tantalizing promise of NCW—the potential to vastly increase capabilities without a concomitant increase in resources.[10]

Unfortunately, networks of specialized units can also be vulnerable to unforeseen or unforeseeable disruptions. Even networks that seem highly resilient can fail abruptly and catastrophically when they suffer unanticipated shocks. Just as the globalized world economy shows the potential benefits of networks and specialization, the worldwide financial crisis demonstrates their dangers.

One portion of the crisis was triggered by the bankruptcy of Lehman Brothers in September 2008, which nearly led to a collapse of the entire world financial system. Tracing the effects of this event in detail illuminates how seemingly trivial linkages in a network can abruptly have enormous effects. When Lehman failed, a money market fund, Reserve Primary, lost $785 million in assets. Banks rely on money market funds for the credit they need to operate on a day-to-day basis, and investors consider these funds to be virtually risk free.[11]

When Reserve Primary took this loss, American money market funds had $3.58 trillion in assets. Investors, stunned that any fund would be so vulnerable, abandoned money market funds en masse. Within a week, banks' access to credit had shrunk by approximately $1 trillion. This threatened to cause further bank collapses, which were only averted by massive government intervention. Thus the initial loss triggered a shift in

Today's military specializes to a degree but has to compromise and retain broader capabilities due to uncertainty.

credit markets that may have been one thousand times as large, and almost caused a mass collapse that was many times larger still.[12]

This enormous swing in the markets was entirely unanticipated because predicting it would have required knowing that: (1) Reserve Primary was so exposed to Lehman that its losses when Lehman collapsed would be unrecoverable; (2) Reserve Primary's losses would trigger a mass panic among other money market funds and the investors in them; and (3) this panic would be of such a scale as to threaten the survival of the world's major financial institutions. The failure of one node triggered failures in connected nodes, which threatened to cause failures in still others. This was a classic cascade failure. The consequences of Lehman's collapse were unknowable because the financial network was so complex that understanding the ramifications of the failure of a single node was beyond the capacity of even the most skilled and knowledgeable experts. It was a classic "Black Swan," an *a priori* unpredictable and unlikely event with huge consequences.[13]

The financial network was vulnerable to a cascade failure partly because many of the institutions comprising it were highly leveraged. Leverage is simply borrowing to increase the total amount that you can invest. Leverage magnifies both gains and losses. In 2004, the Securities and Exchange Commission (SEC) increased the amount of leverage investment banks could use. Previously, the SEC had limited investment banks to a leverage ratio of 12 to 1. They could borrow up to $12 for each $1 in capital they had. The rule change allowed them to increase their leverage to as high as 40 to 1.[14]

Leverage for a financial institution is, in two crucial ways, akin to specialization for a military unit. The first similarity is that both leverage and specialization require making a bet about the future in which increasing the size of the wager enlarges both risks and rewards. A leveraged financial institution is betting that it has assessed future market conditions correctly. If it is right, it will profit far more than it could without leverage. If it is wrong, its losses will be far greater. A specialized military unit is betting that it has focused on the right tasks and that other units will be able to support it if necessary. If it is correct, it will perform far better and far more efficiently than a less-specialized organization. If it is wrong, it risks a catastrophic failure. Think of today's military as being made up of

units like investment banks before the SEC's rule change. They specialize to some extent but still retain a margin for error. Maintaining this margin requires sacrificing some efficiency, just as limiting leverage requires sacrificing some profit. A highly specialized unit, however, would be like an investment bank leveraged at 40 to 1. It might be more efficient, but it would have a much smaller margin for error.

The second similarity between leverage and specialization is that both are only possible within a network and can spread risk through it. A financial institution can take on leverage only if it is connected to other institutions willing to lend to it. Such lending exposes those institutions to the risks assumed by the one doing the borrowing. A military unit can specialize in one task only if it is networked with other units that specialize in different ones and can assist it when required. Both situations, however, highlight a central dilemma of networks. The benefits of the network can only be fully captured if its nodes are reshaped to take advantage of the networked capabilities. Such reshaping will increase the risk of cascade failure if the network's designers have incorrectly forecast the future.

Financial markets are notoriously difficult to predict and can be subject to sudden changes. Predicting the conditions of future battle is no easier. Militaries have great difficulty predicting the characteristics of future wars. This may be a product of the fact that foreign policy experts in general, like their financial counterparts, have little or no ability to predict the future.[15] The more specialized any organization is, however, the less slack capacity it will have to deal with unanticipated contingencies, and the more it will have to transform itself when unpredicted events occur. Architects of the military's future force must thus attempt to capture the benefits of NCW while maintaining the resilience and flexibility of the system in the face of an unknown and unknowable future. Agility within one type of warfare may be of no help to a force attempting to deal with an entirely different contingency.

The Map Is Not the Territory

Perhaps no situation in the business world is more analogous to exercising command in combat than being on a Wall Street trading floor. Both settings involve enormously complicated decisions in an environment of uncertainty, rapid change, information overload, enormous stress, and extreme time pressure. Such an environment puts great pressure on even the best-trained and most capable people and almost always makes them rely, at least in part, on cognitive shortcuts and simplifying assump-

tions. These choices can lead to disaster if their underlying assumptions and implications are not fully understood.

One such shortcut was called the "fallacy of misplaced concreteness" by the influential philosopher and mathematician Alfred North Whitehead. It played a key role in the financial crisis and poses a threat to the network-centric military of the future. The fallacy is captured by the phrase "the map is not the territory." A map is a simplified representation of the territory it describes. A more detailed map is not necessarily a more useful one. More detail provides a closer reflection of reality, but it can also confuse those who do not need such complete information.[16] The fallacy of misplaced concreteness is important because human beings have a powerful tendency to reify symbols by attributing accuracy and power to them that they do not truly possess.

Credit-rating agencies (CRAs) played a key role in the ongoing financial crisis because many financiers fell prey to Whitehead's fallacy. CRAs provide credit ratings which are meant to serve as a neutral assessment of the risk of default. "AAA" ratings convey the lowest degree of risk. Such ratings have enormous influence and often even legal standing. They are never, however, supposed to take the place of an investor's independent judgment. During the lead-up to the crisis, this is exactly what happened. Financial institutions created pools of subprime mortgages, then used sophisticated financial techniques to create new securities based on them. Despite the fact that none of the underlying mortgages was of high quality (hence the "subprime" designation), the CRAs routinely graded these securities AAA, justifying the score by pointing to the sophisticated financial models they had built. Other financial institutions then purchased the securities, using the rating to justify the claim that they were taking on little risk.[17]

The institutions purchasing these supposedly risk-free securities, however, had confused the map with the territory. The rating is a symbol of the risk of default. The actual risk is a far more complex construct based on a variety of variables, including the health of the broader economy. Determining that subprime mortgages were far riskier than their ratings suggested was possible. But many institutions relied on the symbol instead. When these securities began to default, they threatened to destroy the institutions that had purchased them.[18]

The network of the future will present commanders with symbols—abstract representations—of their units that have great superficial verisimilitude. The symbols will be far more realistic than sand tables or paper maps and will be backed by sophisticated computer models that few if any users will truly understand. This apparent fidelity will increase commanders' susceptibility to the fallacy of misplaced concreteness. When

units are symbolized by miniature tanks on a sand table, there is a constant reminder that much information is being lost in the process of depicting them. The loss will be far less obvious when forces are symbolized by sophisticated icons backed by powerful computer models. Command systems drawing upon the information in the network will have powers and flexibility that Napoleon or Patton could never have imagined. The systems will, however, still rely on simplified representations of reality. In the simplification process, by definition, some information is lost. Which information is sacrificed will have been decided by the designers of the network based on their expectations of future combat, years before commanders use the system in battle. Commanders under enormous pressure will be highly susceptible to forgetting the simplifying assumptions underlying the picture presented by the network. This pressure will become ever more acute as new generations of automated systems steadily improve the apparent, although not necessarily the actual, fidelity of their representations.

This temptation may be further exacerbated by the claims of the most-enthusiastic NCW proponents that the network will "surely significantly reduce [the fog and friction of war]."[19] Better networks may well render the battlefield more transparent, but misunderstandings about their limitations may simultaneously introduce new sources of friction.

Even the most sophisticated investors from the most successful firms fell prey to the fallacy of misplaced concreteness, with disastrous consequences. It is unlikely that commanders in combat, operating under far more chaotic and stressful conditions, will be immune to its temptations unless the builders and users of the network pay careful attention to the risk it poses.

The Limits of Simulation

Implementing NCW will require creating sophisticated databases capturing every aspect of the battlefield. These databases might offer the ability to rehearse, model, and simulate potential conflicts with heretofore unimagined levels of speed and accuracy.[20] Commanders of the future might be able to test varying strategies and tactics, refining their plans during dozens or even thousands of practice runs, inserting different enemy actions and random variations until they have developed an ideal approach. This technique could give them unprecedented mastery over the randomness of combat, allowing them to minimize Clausewitzian friction.

Here too the financial crisis presents an example of significant risk. Financial institutions thought that their sophisticated models would permit them to minimize and manage risk, only to have those models fail in a cri-

Unfortunately, networks of specialized units can also be vulnerable to unforeseen or unforeseeable disruptions.

sis, precisely when they were most needed. The false impression of accuracy conveyed by the models meant they too often supplanted the human judgment which might have protected the companies using them.

One of the central tools in financial risk management is Value at Risk (VaR). VaR builds a model of the financial market to measure potential risk to a portfolio. VaR is so influential that the Basel Committee on Banking Supervision has ruled that banks can use VaR to determine the amount of capital they must keep on hand (the more capital a bank has, the safer it is).[21]

VaR, however, has critical flaws. It relies on normal distributions—the bell curve—to model market movements. Unfortunately, markets actually have very large swings more often than the normal distribution predicts. This means that VaR is correct most of the time, but when it is wrong it is very wrong. It also relies on historical data to predict the future. The underlying phenomena that cause price changes in markets, however, can change in ways that have no historical precedents. This risk is absent from the model, and it is hard to imagine how any model would capture it. Defenders of VaR argue that any measure, even a flawed one, is better than no measure. But when VaR fails, it does so when swings in the market are very large, and this instance is when risk management is most needed. Risk management failures during normal times mean losing money. Failures in a crisis can mean losing the company. VaR "is like an air bag that works all the time, except when you have a car accident."[22]

Opponents of VaR further argue that it creates false confidence in its users and so actually makes catastrophic failures more likely. They say that financiers would have been better off with no model, as this would have forced them to use instinct, experience, and their own judgment instead of a flawed computer simulation.[23]

Any military simulation is likely to be at least as susceptible to such problems. Military problems at the operational level and above are nonlinear and interactively complex, making them unsuited to quantitative analysis. Small changes in initial conditions or small adjustments by a combatant can unpredictably result in very large effects. This means that when simulations err they are likely to err by large amounts as the impact of small deviations reverberates through the battle, building on themselves until the predicted outcome has no resemblance to the real one. Future

conflicts are also likely to exhibit significant discontinuities from those in the past for reasons ranging from technological change to tactical innovation to new strategic imperatives. Claims of such a discontinuity are, after all, standard in literature that proclaims the existence of a Revolution in Military Affairs driven by information technology, the very literature upon which the theory behind NCW was built.[24]

Such models and simulations will present an almost irresistible temptation to commanders seeking any possible advantage over opponents. They can be a useful tool. VaR may have provided early warning of aberrant conditions in the market to traders at Goldman Sachs when they combined it with other models and their own experience and judgment.[25] But simulations are useful only when their limitations are fully understood and internalized by their users, and only when they are used as aids to human judgment, not as substitutes for it.

Conclusion

The DOD's movement to NCW is as inevitable as the transition to aerial warfare once was. The promised benefits of the network are so great that they will not be forsaken because of the risks NCW presents. The DOD now has to master the network and learn how to use its capabilities to win future conflicts. Aerial warfare changed militaries' speed, reach, and destructive potential. Network warfare holds the promise of unprecedented speed and accuracy in everything from battlefield awareness and targeting to coordination and command and control. Yet just as aerial warfare is vulnerable to natural hazards and enemy action, network warfare is also fraught with hazards: those its users bring with them and those introduced by the enemy. The first step in overcoming those hazards is a keen awareness of what they are and from where they come.

Military leaders should be sobered by the knowledge that it was not ill-informed amateurs who made the mistakes that contributed to the financial crisis. Highly trained and carefully selected professionals from respected institutions were deceived by the hidden dangers in the world's financial network. As they negotiate their own complex warfighting network, even the best military professionals will need to be both more cautious and more successful than their financial counterparts. Lives and missions will hang upon their decisions while they face a thinking enemy constantly striving to take advantage of every misstep.

Nothing in this article is meant to suggest stopping the pursuit of NCW. Instead, it seeks to reveal unanticipated dangers that the network might present and to recommend a cautious approach to this critically im-

portant work. The following four specific measures could help the American military capture the advantages of the network and mitigate its risks:

• Open debate about NCW, its intellectual underpinnings, the technologies necessary to create it, and the doctrine required to take advantage of these new capabilities will be crucial to successful implementation. The most fervent advocates of NCW have indulged in rhetoric that serves more to stifle debate than encourage it, calling upon the DOD to "root out the resisters and prod the late adopters." No theory should be immune from criticism. Candid, constructive, and honest debate will be far more fruitful than stifling consensus.[26]

• Both supporters and opponents of NCW should tone down their rhetoric. Proponents of NCW should be open to criticism that might improve the theory and be willing to accept that any idea has limitations and weaknesses often more acutely seen by its opponents. Opponents need to accept that the DOD has made its decision, one that cannot, should not, and will not be reversed. Their greatest contribution would be to assist in capturing the benefits and avoiding the dangers of the network-centric approach.

• The assumptions, limitations, and failure conditions of the theories, doctrines, and technologies associated with the creation of NCW need to be explicitly stated and made part of training. Many of the greatest pitfalls created by networks will be obviated if future users understand what the networks are designed to do and what is outside their envisioned use. If users know when they are in domains the designers of the network had not anticipated, they will know to keep the limitations of the system in mind. Cascade failures are a danger, representations of the battlefield may be missing crucial information, and simulations of combat can lead them astray. If future commanders are taught to constantly keep these conditions at the forefront of their minds, they may do better than their financial counterparts at avoiding the risks presented by networked capabilities.

• Most important, the designers and users of the future network will require extraordinary levels of intellectual humility if they are to succeed. They have to appreciate that they probably do not understand all they think they do regarding how people and the network interact, and they may not be able to control even those things which they do understand. Education and training are required to temper the notion that the network will provide an omniscient perspective of the battlefield. There will not be one Common Operational Picture. There will be many pictures, each with its own virtues and limitations. The network will have flaws. Even at its best, it will be an approximation of reality at a moment in time. It will hide as well as reveal. The operators of the future need to understand and respect

the limits of the network with much more sophistication than their counterparts do today. Those who design and populate the network have to be more forthcoming regarding the errors individual pieces of the network may introduce or be vulnerable to, and assist operators in understanding how to overcome those deficiencies. Discussions of error rates and latency should become as prominent as discussions of baud rate and waveforms are now. Caution and humility are not virtues routinely urged upon leaders selected, trained, and promoted for their ability to remain confident and resolute in the face of extreme uncertainty. Yet such behavior will be indispensable to the American military's attempt to profit from the extraordinary capabilities offered by Net-Centric Warfare and avoid being undone by the dangers inherent in it.

These suggestions are not a complete plan for how to counter the possible risks associated with NCW. They are simply a beginning.

NOTES

The authors would like to thank Vice Admiral Nancy Brown, Joint Staff J-6; Lieutenant Colonel Charles J. McLaughlin IV; Colonel John P. Sullivan; Austin Long; Daniel Summers-Minette; and David Warsh for their comments. The National Science Foundation provided partial funding to Mr. Mukunda for this research.

1. John G. Grimes, *Department of Defense NetOps Strategic Vision* (Washington: Office of the Assistant Secretary of Defense for Networks and Information Integration, 2008), http://www.defenselink.mil/cio-nii/docs/DOD_NetOps_Strategic_Vision.pdf.

2. Arthur K. Cebrowski and John J. Garstka, "Network-centric Warfare: Its Origin and Future," *Proceedings*, January 1998; Herbert R. McMaster, *Crack in the Foundation: Defense Transformation and the Underlying Assumption of Dominant Knowledge in Future War* (Strategy Research Project, US Army War College, 2003), 69; Gautam Mukunda, "We Cannot Go on: Disruptive Innovation and the First World War Royal Navy," *Security Studies*, 19 (forthcoming).

3. Donald Rumsfeld, *Quadrennial Defense Review Report* (Washington: Department of Defense, 2006), http://www.defenselink.mil/qdr/report/Report20060203.pdf, 58.

4. Department of Defense, *Net-Centric Environment Joint Functional Concept*, Version 1.0 (Washington: Department of Defense, 2005), http://www.dtic.mil/futurejointwarfare/concepts/netcentric_jfc.pdf, 1.

5. Stephen Biddle, "Victory Misunderstood: What the Gulf War Tells Us About the Future of Conflict," *International Security*, 21 (Fall 1996); John A. Gentry, "Doomed to Fail: America's Blind Faith in Military Technology," *Parameters*, 32 (Winter 2002-03); Richard J. Harknett and the JCISS Study Group, "The Risks of a Networked Military," *Orbis*, 44 (Winter 2000); H. R. McMaster, "On War: Lessons to be Learned," *Survival*, 50 (February/March 2008).

6. David G. Chandler, *The Campaigns of Napoleon: The Mind and Method of History's Greatest Soldier* (New York: Scribner, 1966), 147; US Army Training and Doctrine Command, TRADOC Pamphlet 525-5-500, *Commander's Appreciation and Campaign Design* (Fort Monroe, Va.: Headquarters US Army Training and Doctrine Command, 2008), http://www.tradoc.army.mil/tpubs/pams/p525-5-500.pdf, 8-9.

7. David S. Alberts, John J. Garstka, Richard E. Hayes, and David A. Signori, *Understanding Information Age Warfare* (Washington: DOD C4ISR Cooperative Research Program, 2001), 160-61; David S. Alberts, John J. Garstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority* (2d ed.; Washington: DOD C4ISR Cooperative Research Program, 1999), 55; McMaster, "On War," 26.

8. David S. Alberts, *Information Age Transformation: Getting to a 21st Century Military* (Washington: DOD Command and Control Research Program, 2002); Alberts, Garstka, Hayes, and Signori; Alberts, Garstka, and Stein; McMaster, "On War," 26; Department of Defense, *Transformation Planning Guidance* (Washington: Department of Defense, 2003), 21.

9. Adam Smith, *Inquiry into the Nature and Causes of the Wealth of Nations* (New York: Penguin, 1999); David Warsh, *Knowledge and the Wealth of Nations: A Story of Economic Discovery* (New York: W. W. Norton, 2006).

10. Alberts, Garstka, Hayes, and Signori; Alberts, Garstka, and Stein; Sven W. Arndt, "Super-Specialization and the Gains from Trade," *Contemporary Economic Policy*, 16 (October 1998); Christian Broda and David E. Weinstein, "Globalization and the Gains from Variety," *Quarterly Journal of Economics*, 121 (May 2006); Cebrowski and Garstka; Robert C. Feenstra, "New Evidence on the Gains from Trade," *Review of World Economics*, 142 (December 2006); Paul R. Krugman, "Intraindustry Specialization and the Gains from Trade," *The Journal of Political Economy*, 89 (October 1981).

11. Christopher Condon, "Reserve Primary Money Fund Falls Below $1 a Share," *Bloomberg.com*, 16 September 2008; John C. Doyle, David L. Alderson, Lun Li, Steven Low, Matthew Roughan, Stanislav Shalunov, Reiko Tanaka, and Walter Willinger, "The 'Robust Yet Fragile' Nature of the Internet," *Proceedings of the National Academy of Sciences*, 102 (11 October 2005); Sam Jones, "Wednesday Catastrophe: Breaking the Buck," *Alphaville* blog, 17 September 2008; Sam Jones, "Why Letting Lehman Go Did Crush the Financial Markets," *Alphaville* blog, 12 March 2009; Krugman; Nassim Nicholas Taleb, *Fooled by Randomness: The Hidden Role of Chance in Life and in the Markets* (New York: Random House, 2005); Nassim Nicholas Taleb, *The Black Swan: The Impact of the Highly Improbable* (New York: Random House, 2007); Warsh.

12. Condon; Jones, "Wednesday Catastrophe;" Jones, "Why Letting Lehman Go Did Crush the Financial Markets."

13. Condon; Jones, "Wednesday Catastrophe;" Jones, "Why Letting Lehman Go Did Crush the Financial Markets;" Taleb, *Fooled by Randomness*; Taleb, *The Black Swan*.

14. Julie Satow, "Ex-SEC Official Blames Agency for Blow-up of Broker-Dealers," *The New York Sun*, 18 September 2008.

15. Peter L. Bernstein, *Capital Ideas: The Improbable Origins of Modern Wall Street* (New York: The Free Press, 1992); Peter L. Bernstein, *Against the Gods: The Remarkable Story of Risk* (New York: John Wiley and Sons, 1996); Eugene F. Fama, "Efficient Capital Markets: A Review of Theory and Empirical Work," *The Journal of Finance*, 25 (May 1970); Burton G. Malkiel, "The Efficient Market Hypothesis and Its Critics," *Journal of Economic Perspectives*, 17 (Winter 2003); Burton G. Malkiel, *A Random Walk Down Wall Street: The Time-Tested Strategy for Successful Investing* (New York: W. W. Norton, 2003); Taleb, *Fooled by Randomness*; Taleb, *The Black Swan*; Philip E. Tetlock, "Good Judgment in International Politics: Three Psychological Perspectives," *Political Psychology*, 13 (September 1992); Philip E. Tetlock, *Expert Political Judgment: How Good Is It? How Can We Know?* (Princeton, N.J.: Princeton Univ. Press, 2005).

16. Samuel P. Huntington, *The Clash of Civilizations and the Remaking of World Order* (New York: Touchstone, 1997), 30-31; Alfred Korzybski, *Science and Sanity: An Introduction to Non-Aristotelian Systems and General Semantics* (4th ed.; Lakeville, Conn.: International Non-Aristotelian Library, 1958); Alfred North Whitehead, *Science and the Modern World* (New York: Free Press, 1967).

17. Michael Lewis, "The End," *Portfolio*, December 2008/January 2009.

18. Ibid.

19. Alberts, Garstka, and Stein, 72.

20. Ibid., 167.

21. James Kwak, "Risk Management for Beginners," *The Baseline Scenario* blog, 4 January 2009; Joe Nocera, "Risk Mismanagement," *The New York Times Magazine*, 4 January 2009.

22. Philippe Jorion, "In Defense of VAR," *Derivatives Strategy*, April 1997; Joe Kolman, "The World According to Nassim Taleb," *Derivatives Strategy*, December/January 1997; Kwak; Benoit B. Mandelbrot and Richard L. Hudson, *The (Mis)Behavior of Markets: A Fractal View of Risk, Ruin, and Reward* (New York: Basic Books, 2004); Nocera; Yves Smith, "Woefully Misleading Piece on Value at Risk in New York Times," *naked capitalism* blog, 4 January 2009; Nassim Taleb, "Against VAR," *Derivatives Strategy*, April 1997; Taleb, *The Black Swan*.

23. Taleb, "Against VAR;" Taleb, *Fooled by Randomness*; Taleb, *The Black Swan*.

24. Alberts, Garstka, Hayes, and Signori; Alberts, Garstka, and Stein; Cebrowski and Garstka; US Army Training and Doctrine Command, 6-7.

25. Nocera.

26. Alberts, 15; Darryn J. Reid, Graham Goodman, Wayne Johnson, and Ralph E. Giffin, "All that Glisters: Is Network-centric Warfare Really Scientific?" *Defense & Security Analysis*, 21 (December 2005).