

SSP Working Paper  
May 2003

**Perfect Information and  
Perverse Incentives:  
Costs and Consequences  
of Transformation  
and Transparency**

**Michael Schrage**

Michael Schrage is a senior advisor to MIT's Security Studies Program and co-director of the MIT Media Lab's eMarkets Initiative and works closely with several commercial 'net-centric' organizations

**The Security Studies Program (SSP)** is a graduate level research and educational program based at the MIT Center for International Studies. The Program's primary task is educating the next generation of scholars and practitioners in international security policy making. Its teaching ties are mainly, but not exclusively, with the Political Science Department at MIT. However, the SSP faculty includes natural scientists and engineers as well as social scientists, and the Program is distinguished by its ability to integrate technical and political analyses in studies of international security issues. The SSP faculty, several of whom have had extensive government experience, frequently advise or comment on current policy problems. SSP supports the research work of graduate students, faculty and fellows, and sponsors seminars, conferences and publications to bring its teaching and research results to the attention of wider audiences.

## **Abstract**

This paper argues that the benefits of information superiority in attaining military superiority may be vastly overestimated. The economics of ‘information-rich’ environments inherently inspire perverse incentives that frequently generate unhappy outcomes. The military must rigorously guard against the threat of ‘diminishing returns’ on its net-centric investments. Drawing on the author’s private sector experiences with net-centric transformations, several approaches for reassessing the military value of information transparency are suggested.

## **Author’s Note and Acknowledgements**

This paper was completed barely six weeks before the launch of the second Gulf War in Iraq. It is being released after the formal end of declared hostilities. Much to my relief, the thrust of the argument remains valid. (In the interests of intellectual integrity, I did not alter the paper to reflect any ‘lessons learned’ from the campaign). America’s information superiority undeniably played a critical role in attaining a swift military victory. Then again, several of the pathologies described in this paper did play out in “Iraqi Freedom.” As real-time intelligence, analysis, damage assessments and operations become even further integrated, the issues identified in this paper will grow in importance for both planners and policymakers.

One aspect of the recent campaign totally – and wrongfully – left out of this paper was the role of Special Forces in shaping the battlefield. While a detailed description of Special Forces impact on this Iraq War may never fully be known in the open literature, I would argue that their role was analogous to high-risk/high-reward venture capitalists and entrepreneurs in the ‘military marketplace.’ Special Forces completely and utterly changed the ‘risk profile’ for the more conventional Army, Navy, Air Force and Marine operations that followed. In other words, Special Forces were a critical ‘risk management’ investment made by the CINC. In ‘portfolio management’ terms, they represented the ‘speculative investment’ that paid off in a huge way. The war might have proceeded quite differently if the return on the CINC’s Special Forces investment had not been so high.

The origins of this paper can be traced to a request by Robert Buder – the author of a superb book on the history of radar – to have me review two national security related books for MIT’s ‘Technology Review’ magazine back in June 2000. Bill Owens’ *Lifting the Fog of War* and Scott Snook’s *Friendly Fire* provoked me into taking a serious look at how America’s military should manage the incredibly high expectations associated with high technology. My September 2000 review ultimately led to this working paper.

This paper unambiguously benefited from review and remarks from Robert Leonhard, the Office of Net Assessment’s Barry Watts and Andrew May, the National Security Council’s Gregory Rattray, MIT’s Harvey Sapolsky, Army special assistant Tom Kelly and Raymond Christian of the Naval Undersea Warfare Center. Special thanks to Stanford University’s Sam Savage for his ongoing insights into ‘risk management.’ Kristen Cashin’s patient editing was also crucial. I am grateful.



## **Perfect Information and Perverse Incentives: Costs and Consequences of Transformation and Transparency**

September 28, 1998 is a date of no great military significance. In global finance, however, it is a day that will live in infamy forever. That day, a U.S. government-supervised consortium of banks bailed out Long-Term Capital Management (LTCM); a hedge fund whose highly-leveraged multi-billion dollar trading losses had put the entire world's financial system at risk of a meltdown.

LTCM's spectacular demise was particularly noteworthy because the firm had been regarded as both paradigm and paragon of a globally successful hedge fund. Funded by many of the most prestigious names in finance, LTCM featured two Nobel laureates as partners. The firm's founders had superb track records on Wall Street. Its trading personnel were a supremely well-educated elite.<sup>1</sup>

Indeed, LTCM's traders saw themselves as financial warriors waging high-tech combat in investment theaters around the world. They relied upon stealth, speed and the ability to execute timely trades 24/7. To accomplish this, the firm made enormous investments in state-of-the-art digital infrastructure. In fact, LTCM relentlessly pushed and prodded their technologies for marketplace advantage. The firm modeled, simulated and computationally stress-tested financial strategies before launching its precision market strikes. These investments seemed to pay off.

By any reasonable standard, LTCM represented precisely the sort of transformational, information-intensive and net-centric organization that America's armed services say they need to become. Any carrier group or Rangers battalion would be thrilled to have the kind of real-time analytics that elite financial trading desks enjoy. At least one highly respected Marine commander appreciates the parallels: he set up trading pit training sessions for his fast-track officers to expand their boundaries of data-driven 'situational awareness.' In effect, the Pentagon's Revolution in Military Affairs (RMA) could profitably benchmark Finance's RMA – the Revolution in Monetary Acquisition.

The analogy is hardly perfect. Hedge funds have neither AWACs nor JSTARS. Soldiers fight for their buddies; traders fight for their bonuses. Military commanders are more concerned about 'collateral damage' than traders. Investors and commanders have profoundly different Measures of Effectiveness (MOEs). But the similarities here are more than merely technological or metaphorical.

Both groups engage in ongoing risk assessment. Both observe highly regulated 'rules of engagement' subject to legal oversight. Digital technology is used to track decisions as well as facilitate them. Both groups 'take positions.' Where the services have 'doctrines,' hedge funds have 'investment philosophies.' Both rely heavily on timely 'intelligence' while confronting deception and disinformation. Both groups coordinate international coalitions and joint operations. Bold leadership, individual initiative and discipline are culturally celebrated core values. Character and esprit matter.

## Transparently Obvious

Hedge funds have at least one huge operational advantage over their military counterparts. No Clausewitzian ‘fog of transaction’ hangs over global trading desks. To the contrary, financial markets worldwide are explicitly designed to be transparent and responsive in ways that military battlespaces can never be. On most every dimension of quality, integrity, comprehensiveness and detail, historical financial data are clearly superior to comparable military data. Financial data, unlike most military data, come in forms and formats that lend themselves to robust net-centric application. Indeed, quantitatively sophisticated hedge funds like LTCM are designed to get greater ‘bang for the buck’ and ‘bang for the bit’ from their information infrastructures.

In theory, network technologies should be ‘force multipliers’ for these data-driven traders. In the real world, however, IT all too frequently becomes a ‘force divisor’ undermining both strategic intent and tactical execution. ‘After action reports’ detailing the transformational pathologies of LTCM’s collapse might prove even more enlightening to the Office of the Secretary of Defense (OSD) and the Joint Chiefs of Staff (JCS) than for the Federal Reserve. Even today, there’s no professional consensus explaining why LTCM imploded as it did. But nearly every serious assessment agrees that the size, speed and breadth of the fund’s collapse defied the rational expectations of the time. Even the surprise was a surprise. That’s one reason LTCM offers a vital case study in net-centric failure.

While not typical, LTCM’s story is hardly unusual. Since the global stock market peaks of 2000, a statistically significant number of the most highly-regarded, net-centric hedge funds have dramatically underperformed diversified index funds.<sup>2</sup> This record of financial underperformance extends to other industry sectors that claim significant competitive advantage from their net-centric investments.

For example, Cisco Systems - popularly described as a well-managed high-tech firm with a superb digital nervous system - was forced to take a \$2.25 billion inventory quarterly write-down in Spring 2001.<sup>3</sup> This multibillion dollar hit was one of the largest in U.S. corporate history. Alas, Cisco executives had bragged to the Harvard Business Review that its tracking systems were so sophisticated it could ‘close the books’ on its quarterly earnings in under three days. Indeed, Cisco’s top executives repeatedly assured investors the company deserved an equity premium in part *because* its data-driven operational controls were so good.

Was Cisco’s multibillion dollar mistake an aberration? Analysts say not. The presumed excellence of Cisco’s information systems invited managerial over-reliance. Over-reliance bred overconfidence. Cisco’s top executives chose to minimize or ignore unambiguous external market signals in favor of their own networked data. No Information Age cliché of ‘garbage in/garbage out’ here; Cisco’s debacle - like LTCM’s - occurred despite a world-class corporate communications, command and control system.

There are scores of comparable failures. Indeed, such examples are likely underreported by firms not wishing to call attention to their mistakes. But any objective review of private sector experiences with digital transformation offers RMA champions evidence more sobering than inspiring. The potentially enormous benefits of net-centric transformation should be valued only in the context of their potentially enormous costs. These cost-benefit ratios have not been adequately assessed. The fundamentalist dogma of the RMA transformation ideology recalls the aphorism, “Be careful of what you want because you’re sure to get it.”

## **Dogma Driven Data**

The problem, ironically, has nothing to do with mediocre people mismanaging mediocre systems. Mediocrity drives neither military nor marketplace dominance. Excellence does. Perversely, the most technically sophisticated net-centric firms have often proved to be most vulnerable to the inherent pathologies of data-driven mismanagement. These are failures of excellence. World-class ‘information intensive’ infrastructures can actually amplify, accelerate or induce devastating professional misjudgments. Fund managers “knew” that there were speculative bubbles in the internet, telecom and biotech sectors. They invested anyway. Having the ‘right’ information at the ‘right’ time may not lead to the ‘right’ decision.

Although financial markets are far more transparent than battlefields, even the most elite net-centric firms can’t reliably count on ‘information superiority’ to generate superior returns. They can’t even count on ‘information superiority’ to prevent catastrophic losses. Similarly, even the most elite military units can’t reliably count on ‘information superiority’ to generate superior mission effectiveness. Nor can they count on ‘information superiority’ to prevent catastrophic mission failure. The same risk management pathology that afflicts financial cyberspace will invariably afflict information-based military initiatives.

The conclusion? Information is vastly over-rated as a military asset. Greater operational transparency does not guarantee greater military effectiveness. Attributing the benefits of networked *technologies* to the virtues of net-centric *organization* distorts reality.

Military doctrines based on the assumption that quantum leaps in the quantity, quality and timeliness of information will radically enhance tactical and strategic decision-making are inherently flawed. These doctrines are as flawed as ‘killer app’ business plans promising greater profitability if only firms reorganize themselves around innovative information-intensive networks.<sup>4</sup>

Even when very smart, very motivated decision-makers are presented with near-perfect information, they consistently sub-optimize. Indeed, an entire discipline of ‘behavioral economics’ has arisen to explain why individuals and institutions exhibit seemingly non-rational - and counter-productive - investment behaviors.<sup>5</sup> Military commanders are no less susceptible to these non-rational behaviors than professional investors. This paper explains why.

## **Fog? What Fog?!**

Transformational doctrines can’t live up to the lofty expectations of their champions. We need to fundamentally rethink the role of information abundance in military decision-making.

Consider the following thought experiment: Breakthrough technology effectively lifts the fog of war. At any time, a Commander-in-Chief (CINC) can see any part of any theater at any degree of resolution he desires. Multi-spectral, multi-perspective systems enable real-time assessments of thermal and visual status of combat from a variety of angles. Enemy movements are as transparent and accessible as friendly positions. Satellite suites and networked drones instantaneously let commanders see if Precision Guided Munitions have destroyed their targets. Immediate voice and/or data communications with any individual, unit or platform are crisp. Communication systems are fully inter-operable. Unit commanders are jacked into battlennets allowing any level of situational awareness they desire or that the CINC permits. Any officer can get any piece of real-time data they need whenever they need it.

So how much of a force-multiplier would this best case information-rich scenario be for the U.S. military?

The only honest answer is: It depends. But if economic logic, empirical observation and active experimentation are any guide, there is every reason to believe that ‘fog-free’ battlefields would just as easily undermine politico-military effectiveness as enhance it. Even if perfect battlefield transparency could be achieved for ‘free,’ its costs might well outweigh its benefits.

“When we began large-scale experimentation in information operations in the army, many of us expected that better visualization of the battlefield would result in more efficient engagement of the *critical* pieces of the enemy array, and, therefore, a greater economy in terms of ammunition requirements,” writes army officer Robert R. Leonhard in his superb *Principles of War for the Information Age*. “It seemed intuitively obvious to me that greater accuracy - both in technical and operational terms - would result in fewer required missiles and short tons of ammunition. Imagine my surprise when the experimental units required *five times* the ammunition they used to expend!”<sup>6</sup> Suddenly overwhelmed with the vast array of potential targets that they could now see, the experimental units pleaded for more ammunition.

“This unprecedented need for large, expensive quantities of ammunition caused logistical nightmares...,” he recalls. More information - better information - did not assure better decision-making. It exposed doctrinal flaws.<sup>7</sup>

### **You Can’t Be Too Rich O.R.**

The Information Age truism that, “Knowledge is Power” does not seamlessly scale into “More Knowledge is More Power.” Why not? Because the economics of information in war create perverse incentives. These perverse incentives pose enormous risks for battlefield commanders and their civilian overseers. Perverse incentives guarantee perverse outcomes.

Better managing information economics - not just better managing information - is what will ultimately determine the efficacy of America’s RMA initiatives and net-centric transformations. RMA advocates must recognize that quantitative changes in information and analysis invariably lead to qualitative changes in individual and organizational behavior. Many of these behaviors will be ‘rationally counter-productive.’

This critical observation has nothing to do with legacy notions of ‘information overload’ and everything to do with ‘diminishing returns.’ The national security implications of ‘diminishing marginal utility’ were brilliantly discussed both in Hitch and McKean’s classic *The Economics of Defense in the Nuclear Age*, and Enthoven and Smith’s subsequent *How Much is Enough?*<sup>8</sup>

Their core argument was that ‘systems analysis’ - a microeconomics-based reinterpretation of World War II’s ‘operations research’ - should help decision-makers frame quantitative trade-offs around their national security investments. Their key assumption was that normative systems analysis methodologies would indeed yield ‘efficient frontiers’ and ‘optima’ for assessing the cost-effectiveness of various weapons systems.

But where the budget-conscious Hitch and Enthoven systems analysts asked, ‘What added effectiveness does that additional dollar buy?’, the data-conscious post-industrial RMA advocate must upgrade the question to:

‘What added effectiveness does that additional information buy?’ In other words, what is the marginal return on information? How do we know?

The nature of information - and information economics - makes answering those questions unusually challenging. Why? Because dollars aren’t data. Budgetary dollars may be scarce but battlefield information grows ever-more abundant. A CINC, forward air controller or battlefield commander may receive anywhere from 10 to 1000 times more information per unit time to make decisions. Managing this abundance poses different economic challenges than managing scarcity. What does an ‘efficient frontier’ or ‘optimum’ look like for a resource that’s continually becoming better, faster and cheaper? Net-centric technologies offer digitized warriors a continual embarrassment of riches. But how do markets value ‘gluts’?

Traditional economic theory asserts that exponentially growing resources invariably become *less valued* over time. They become commoditized. The more bullets you have, the less valuable they seem. The notion that faster, better and cheaper information could be seen as less valuable may seem perversely counter-intuitive. But economic history teaches that organizations tend to squander their cheapest resources. In World War I, the abundance of conscripts made sacrificing young soldiers easier than it might have been. ‘Replacement costs’ were not seen as unduly high. There would always be other young men. Perhaps a digital Douglas Haig cavalierly wasting bits and bandwidth instead of human lives might strike military historians as representing genuine progress. But if squandering battlefield information ultimately leads to unnecessary loss of battlefield lives, then that progress is marginal at best.

### **More Information = More Analysis**

The history of financial markets affirms: an exponential increase in information supply assures a dramatic rise in analysis demand.<sup>9</sup> Unless the overwhelming majority of that additional information is redundant - in which case its marginal utility rapidly plummets - its value is largely contingent upon the quality of analysis. In other words, a surging abundance of information inherently highlights a sudden scarcity in analytics. Bringing them into equilibrium is expensive.

In finance, the real-time transactions data tsunami has driven extraordinary investment and innovation in quantitative analytics. Financial analysts perform ever-increasing varieties of multivariate regressions to identify useful correlations. Financial engineers run tens of thousands of Monte Carlo simulations in the course of designing synthetic securities or risk-sensitive portfolios. The more financial information there is, the greater financial analysis needed. Crucial divisions of labor emerge between traders, analysts and financial engineers. Coordination costs increase. Interdepartmental disagreements over perceived risks intensify. Conflicts between analysis and operations become acute.

Lifting the fog of war triggers a comparable surge for military analysis. Dramatically more information means dramatically more power and influence for analysts. How could it not? When situational awareness questions mutate from ‘What information do we have?’ to ‘What does this information mean?’, it’s clear that ‘better’ analysis is essential to the answer. ‘Better,’ alas, is relative.

The perverse consequence of the transparent battlespace is that it confuses rather than clarifies where these analyses should take place. One argument is that transparency and net-centricity turn theater conflict into a centralized virtual video game for the CINC and his staff. The CINC literally sees ‘The Big Picture’ and can

prioritize initiatives and responses accordingly. To be sure, the CINC is ultimately held accountable. But does that mean centralized analysis represents the optimal mechanism to manage the information onslaught?

Alternately, the CINC can 'delegate' to his service commanders and let them customize analysis for their particular needs. Then again, some RMA champions assert that greater information transparency should explicitly translate into greater empowerment for unit commanders and their charges. They contend that greater situational awareness is a tremendous motivator and force multiplier. They say CINC's must be prepared to incorporate bottom-up initiatives as well as issue top-down commands. This was clearly demonstrated by the improvised effectiveness of Special Forces/Air Force co-operation in the Afghanistan campaign. After all, superbly-trained soldiers, sailors and airmen shouldn't be mere multi-media-manipulated 'meat puppets.' So what is the appropriate locus of empowerment?

This simply recapitulates the classic centralization/decentralization dichotomy that haunts organizational design. Net-centricity and information transparency combine to create a managerial challenge unknown to either traditional military command and control hierarchies or decentralized special operations. In practice, this techno-fusion allows the CINC to simultaneously centralize and decentralize his command. He can see everything; alternately, any other commander, in theory, could have access to any information necessary to enhance mission effectiveness. The 'chain of command' becomes a de facto 'network of command.'

Of course, the CINC could choose to deny unit commanders the information and/or analytic access they say they need. That's a judgment call. But the choice to deliberately withhold information has potentially profound implications for unit cohesion, trust and morale. Commanders denied 'information reinforcements' by a CINC for mission-critical analysis may understandably feel undermined.

But if - as is usually the case - distributed military analyses generate fundamentally different interpretations of events, then more analyses inherently mean more disagreements. Lifting the fog of war invariably intensifies dueling analyses that are based on common information. Analytical disagreements over data interpretations are common. This situation is uniquely different from the past because, ostensibly, more commanders have more immediate access to more information.

If they don't, then the RMA is really nothing but a revolution in the recentralization of command. The ultra-centralized CINC then becomes explicitly incented to present analysis that justifies his decisions. In fact, he now has incentive to conceal the more controversial elements of that analysis from his subordinates. That result completely undermines the declared rationales for 'information-based' warfare.

In other words, vastly more information and vastly more analysis in networked commands creates a diversified marketplace for decision. Information-rich net-centric infrastructures make it just as easy to centralize as distribute these command decisions. Indeed, distributed analyses virtually guarantee ongoing competition about who is best situated to interpret events and act upon them. Cultural issues - different service perceptions of risk and reward - intrude. Unsurprisingly, these kind of net-centric conflicts have shattered many of the world's top trading desks.

### **More Information Incentives More Mission Creep**

Further complicating the organizational impact of net-centric warfare is America's tradition of civilian control of the military. A CINC or Secretary of Defense might not like it, but there is no technical reason why an Administration's human rights lawyers and refugee response administrators couldn't be connected to situation rooms to monitor relevant military decisions. International law and military conventions could, in fact, ultimately require such real-time civilian oversight.

If a major objective of a military campaign is to effect 'regime change' and facilitate transition to a 'friendly' government, then real-time coordination with humanitarian and civil reconstruction agencies might become part of a CINC's analytical infrastructure. To the extent that military missions are inextricably entwined with humanitarian concerns, then battlespace transparency and net-centricity create a data-driven bias to confronting post-conflict issues ever earlier in the military decision cycle. If war is, indeed, the extension of policy by other means, then 'information-based warfare' becomes the extension of policy analysis by other means.

For example, unmanned aerial vehicles (UAVs) and satellite surveillance determine that a key military target has a greater proportion of innocent civilians than anticipated. The military objective remains paramount but this knowledge alters the options for mission accomplishment. What command level appropriately determines whether the mission should proceed as planned or whether it should be significantly changed? Arguably, the rise of increasingly detailed knowledge of civilian presence in target locations suggests either



*Predator UAV*

dramatically new protocols for notification prior to a lethal strike or - more provocatively - the increased deployment of so-called 'non-lethal' weaponry. Better information invites better reconsideration of the original mission requirements.

Robert Leonhard describes the new choices created by new information as 'options acceleration.' That is undeniably true. But one CINC's 'options acceleration' is another commander's 'mission creep.' In practice, new information isn't merely used to achieve mission objectives, it is often used to *redefine* mission objectives. Investors who acquire valuable new information frequently change their investment objectives precisely because they now have a good reason to alter them. More information makes more investors more opportunistic. Perceptions of the value of information fundamentally shift.

In finance, the economist J.M. Keynes exquisitely described how this phenomenon plays out as new information transforms investors into speculators: "As the organization of investment markets improves, however, the risk of the predominance of speculation does... increase. It is rare...for an American to invest 'for income;' and he will not readily purchase an investment except in the hope of capital appreciation. This is just another way of saying that... the American is attaching his hopes, not so much to its prospective yield, as to a favorable change in the conventional basis of valuation, i.e. that he is, in the above sense, a speculator. Speculators may do no harm as bubbles on a steady stream of enterprise. But the position is serious when enterprise becomes the bubble on a whirlpool of speculation."<sup>10</sup>

Emerging patterns or serendipitous opportunities inherently increase in these information-rich, analysis-opulent military environments. Temptations for mission creep would abound. Consistently resisting those temptations would value discipline over opportunity. Conversely, exploiting increased opportunity would suggest a looser and less rigorous mission definition. Either emphasis increases the chances for perverse consequences.

Factor in the humanitarian, legal and/or policy participation in this data-driven 'options accelerator' and it's blindingly clear that the tempo of reassessing objectives may only slightly lag the increased tempo of combat. That may be a boon for civilian oversight but the stresses that puts on operational commands would be enormous.

The obvious pushback to this organizational threat would be to constrain such civilian interactions and use 'effects-based' military doctrines to strike a balance between mission focus and flexibility. Unfortunately, lifting the fog of war makes that extraordinarily difficult because. . .

### **More Information Imposes More Accountability**

In finance, transparency is the essential ingredient for accountability. In financial regulatory circles, the most vicious battles almost always revolve around disclosure. The more transparent investments are, the more accountable investors are. The more transparent the enterprise becomes, the more accountable management becomes. Verification increasingly substitutes for trust.

Similarly, military transparency and net-centric commands can create excruciating levels of accountability. Recent 'friendly fire' incidents in Afghanistan show just how extensively operational decisions can be captured and critiqued.<sup>11</sup> Everything that matters - and more than a few things that don't - are recorded. The

military's ability to playback and review critical decisions made in real-time has improved by orders of magnitude since the first Gulf War. Battle plans, simulations, war games and OR analyses are digitally archived. In theory, the services and their civilian overseers know who made what command decision when. They know who planned what missions at what level of detail when.

As the world's sole hyper-power, America's national security establishment becomes ever more PC. This PC doesn't stand for 'Politically Correct' but 'Prevent Casualties' and 'Protect Civilians.' Failures of military initiatives to minimize casualties or protect civilians becomes transparent. These failures can and will be digitally second-guessed by both military and civilian review. In an information-rich military environment, forensic strategists and tacticians will almost always be able to uncover data or analysis that conclusively explains why the plan should never have been undertaken in the first place. Commanders "should have known" that those emplacements would take too long to overrun; or that women and children were being held hostage in the ministry; or that anti-helicopter rocket propelled grenade batteries were lying in wait. The ability to 'demonize' or merely politicize flawed military decisions becomes easy.

Accountability concerns further intensify as precision weaponry improvements and information improvements become co-dependent. The marriage of information and precision dramatically elevate performance expectations. Calibrating the level of lethality appropriate to the target consumes a greater analytical consideration. Should a weapon only take out a room instead of a floor? A floor instead of a building? A building instead of a block? What additional information would have made a non-lethal strike the appropriate choice? Why couldn't we get it?

The circular error probabilities or margins of error deemed acceptable in these contexts - 5%? 10%? 25%? Are those margins determined by doctrine or on a mission-by-mission basis? Similarly, what happens when soldiers know that every bullet they fire is being tracked by their 'smart rifles' and special 'battle damage assessment' drones? Do they become more conservative or would they err on the side of aggressiveness?

The audit trails created by these kinds of analyses create a level of accountability unheard of in civilian professional life. Yet ongoing technical trends accelerate the accountability trends. U.S. technology is so superior that it becomes easy to imagine America's more sensitive allies arguing that the U.S. military is ethically – if not legally - obligated to make its smart weaponry even more discriminating. The logical - if ad absurdum - extension offspring of this marriage is targeted assassinations. The Israeli experience in this regard, of course, has been decidedly mixed.<sup>12</sup>

Just as in finance, the rise of transparency creates perverse incentives for military decision-makers to take refuge in deliberate ambiguity, outright concealment and 'cover your ass' risk-averse behaviors. Individual accountability gets blurred into institutional accountability. But where flawed decisions may cost investors money, they can cost commanders the lives of their people and innocent civilians. An ambitious politician or Judge Advocate General or journalist may turn legitimate questions of 'accountability' into inappropriate accusations of 'blame.' How will military cover-ups be managed in the era of fog-free war? Rigorous analysis and combat complexities will *always* indicate another rational path that deserved serious consideration.

## **Mutually Assured Deception**

Cover-ups are deceptions. By its very nature, an increased reliance on better information creates powerful incentives for better deception. In business and finance, deception has long been an intrinsic part of marketplace speculation and investment. Successful marketing of questionable IPOs (initial public offerings) and the misrepresentation-driven bankruptcies of high-flying market leaders like Enron and WorldCom reflect that reality. Executives and their professional advisers frequently ‘game’ accounting rules and regulations in ways that enrich themselves at the expense of their shareholders.<sup>13</sup>

Many financial frauds and business deceptions are unethical; some are illegal. But even in an era of high-tech accounting and financial reporting regimes, deception remains an appealingly effective short-cut to riches. Of course, in business and finance, deceptive practices and frauds are supposed to attract regulatory attention and legal sanction. Outright deception in finance is officially discouraged - although short sellers and traders have been known to plant misleading information in the media and elsewhere. In warfare, however, deception and disinformation are considered essential competencies. There is no international law against them.

The strategic role of deception in warfare goes back to Sun Tzu. Deception and disinformation have played a major role in virtually all significant military conflicts. To the extent that military plans and doctrines are based on superior information assets, the enemy’s incentive to deceive and misinform skyrockets. The military principle of turning an enemy’s greatest strength into his greatest weakness is classic.

Intriguingly, deception in digital domains is significantly less expensive than deception in the physical ones. The economics of deception are inviting. Creating ‘Trojan horse’ computer viruses, for example, is significantly less expensive than building real Trojan horses. Even the most sophisticated sensors can be confused or misled by relatively inexpensive devices. During the Kosovo conflict, drones frequently misidentified wooden decoys as tanks and metal tangles as mortars and machine gun embankments. Skillfully lit fires can mislead thermal sensors and night vision scopes. Indeed, at least one Serbian ruse led an F-16 into a surface-to-air missile trap where it was destroyed.<sup>14</sup>

The co-evolution of measure/countermeasure escalation in technology-driven deception is one of the touchiest topics in modern warfare. In World War II, for example, the British long delayed the deployment of ‘Window’ [chaff]- thin aluminum strips that would create a blizzard of electronic snow on Nazi radar screens - for fear that the Luftwaffe might use such techniques to neutralize Britain’s own Chain Home radar network. The history of electronic warfare is the history of a race between ever more expensive measures being conjured up against ever-cheaper countermeasures.<sup>15</sup>

In a transparent battlefield that can link to global communications networks like CNN, the BBC and Al Jazeera, incentives for increased deception become truly perverse. An elementary school might be made to look like a military barracks in hopes of inducing a humanitarian disaster. A fleet of Red Cross ambulances might be used to transport chemical and biological weapons. Mosques might be used as storage facilities for missile launchers. The incentive to blur clear distinctions between civilian and military targets becomes overwhelming. Portraying civilians as combatants and combatants as civilians is, bluntly, a rational response to technologies explicitly designed to reliably discriminate between military and non-military targets. In other words, seeing is no longer believing. Lifting the fog of war now requires renewed efforts to sort the real targets from the decoys; the real soldiers from the civilians. Of course, this is do-able. But the cost in

time, technology and mission-effectiveness is unknowable in advance. The purpose of deception is emphatically *not* to win a conflict but to dramatically increase the uncertainty of precision military initiatives. To paraphrase Secretary of Defense Donald Rumsfeld: while the absence of evidence may not be evidence of absence - the presence of evidence may not necessarily be evidence of presence. Deception thus becomes a force multiplier.

In effect, information-based transformation doctrines assert that deception merely increases the friction - not the fog - of war. But truly effective deception undermines the RMA premise and promise that net-centric warfare leads to 'safer' and more surgical military strikes. Undermining the military's credibility undermines military effectiveness. Undermining military effectiveness undermines the ability of policymakers to rely on focused military power to attain their professed objectives.

### **Irreducible Uncertainties**

Perhaps the most disconcerting aspect of reviewing the history of operations research and intelligence from World War II on is how little professional consensus there is about the military impact of quality information. Sixty years later, military historians still debate the effectiveness of strategic bombing in World War II. The Strategic Bombing Survey remains a controversial document.<sup>16</sup> Heated arguments continue over how effective interdicting transportation networks and/or petroleum refineries have proven in reducing enemy logistical capabilities.<sup>17</sup> Does 'better' information resolve these historical issues? Apparently not. History obfuscates as often as it clarifies.

For example, revisionist historians sharply question the role of Ultra and Enigma in shortening World War II. They argue that Bletchley Park's ability to read Nazi transmissions did not have either the strategic or tactical impact that was desired.<sup>18</sup> Indeed, the economics of decryption convey the most awkward perverse incentive of all: even if you know exactly what the enemy plans to do, you must limit your response lest the enemy know that you've broken its codes. [Indeed, rumors linger still that operations research (OR) was little more than a cover story to explain the growing Allied success in destroying the Doenitz's Wolfpack.]<sup>19</sup> Perfect knowledge can prove a politico-military liability. Decades after the memoirs and the memos - divorced from the pressures of real-time analysis - even the most intimate participants disagree over cryptography's influence over strategy.<sup>20</sup>

More recently, analysts and flag officers still debate the role of bombing in the Kosovo campaign in inducing the Serbian surrender.<sup>21</sup> Similarly, military experts dispute whether the Tora Bora campaign to track Bin Laden in Afghanistan would have been more successful if there had been greater reliance on American troops instead of local Afghani warlords.<sup>22</sup>

A litany of historical disputes persist over which 'schwerpunkts' really made the difference in a conflict and which ones were merely 'schwachpunkts.' Understanding the role of historical revisionism is essential here precisely because our analytic techniques and computational technologies have grown so much more sophisticated. Despite dramatic improvement, these conflicts over conflicts remain largely unresolved. The revisionist battle lies less over the disputed data than its interpretation.

Intriguingly, this troubled revisionism appears shockingly similar to the efforts made by financial historians to 'explain' the Stock Market Crash of 1929, the Dow's October 1987 500+ point drop or the more contemporary internet/telecom bubbles. The historical record for these events is superb. Yet, clearly,

irreducible elements of chance and contingency have emerged that defy deterministic explanation. Information doesn't adequately resolve these debates; it simply gives more ammunition to the disputants.

The obvious point must be made: even with 20/20 hindsight, many of the world's most important military decisions do not lend themselves to information-based rational analysis. 'Irreducible uncertainties' preclude analytical explanation. Luck matters. The respective roles of 'chance vs. design' prove as obscure in the rigorous review of military campaigns as they have in the post mortems of failed investment initiatives.

While it's unfair to say that military doctrines experience 'random marches' the way financial theory confronts 'random walks,' it's not unfair to observe that military theorists and their financial counterparts are predisposed to believe that greater information can reduce the role of chance in influencing outcomes. That belief reflects more irrational exuberance than rational analysis. The fact that one can load the dice doesn't mean that, in the final analysis, they aren't dice. Trend is not destiny; neither is probability.

To be sure, tremendous analytical success stories exist. The classic Blackett's Circus OR tales of convoy size and depth charge settings immediately come to mind.<sup>23</sup> Unfortunately, the quantitatively trained military historian has a sample bias issue with those analyses. What are the ratios between analysis that made things better, made things worse and had no measurable impact at all? The studies detailing the impact of flawed OR analyses by Blackett's Circus or Morse's ASWORG or Leach's 8th Air Force operations analysis unit have yet to be written. By contrast, a distrust of formal analytics is surely one of the horrific military legacies of Viet Nam. Perverse MOEs simultaneously undermined both military morale and civilian support. The ironic conclusion that military cost/benefit analysis may not consistently prove cost beneficial is tempting beyond endurance.

### **Inform(ation)al Conclusions**

The peculiarities, perversities and pathologies of information economics afflicting elite financiers when they make investment decisions cannot be glossed over or ignored by commanders as they increasingly rely upon 'better' information to make military decisions. The world's savviest investors lost tens of billions of dollars when the Internet, tech and telecom bubbles simultaneously burst. Where was the shortage of information just before that implosion? Who didn't know that their portfolio companies were trading at infinity times earnings? Which investors didn't observe both analysts and CFOs conjuring up new rationales to explain absurdly high valuations? With both their reputations and their fortunes at stake, the world's 'smartest' and 'boldest' professional investors bid up bubbles that ultimately popped. Investment amateurs were massacred, too. Yet both groups couldn't have had a more transparent battlefield.

While stock market bubbles have no direct analogy in military affairs, the frenzy of mismanaged expectations is hardly unknown during wartime. At the heart of every speculative frenzy is the honest but misguided belief that a commodity is far more valuable - and will continue to be far more valuable - than either history or rational analysis can reasonably support.



*PMS Blackett, the "father of OR"*

Both history and logic strongly indicate that reaping value-added military advantage from information superiority is not a given. The National Security establishment, the Intelligence Community and the Armed Services are woefully underinvested in appreciating the risks associated with data-dependent military doctrines. RMA discussions have overwhelmingly focused on information's rewards.

An unflinching and intellectually honest approach to the value of information requires the explicit recognition that a rigorous form of 'portfolio management' is required. Modern Portfolio Theory, Bayesian analysis and Monte Carlo simulation are just three of the more obvious quantitative tools that military decision makers must grasp if they want the benefits of transparency to consistently outweigh its costs. If 'information' were to be managed as a portfolio of investment risks much as asset classes like equities, fixed income and commodities, how would CINCs and commanders diversify to maximize their returns? What 'information asset classes' would they deem most volatile? What information would they see as most reliable? Which 'information classes' would be co-variant? Which would be auto-correlated?

The 'modern portfolio theory' approach is particularly pertinent to 'information asset management' because it offers a constructive way to assess key risk-management trade-offs. For example, financial portfolio theory argues that a mere millionaire would be foolish to make significant investments in venture capital. By contrast, a billionaire would be foolish *not* to make significant venture capital investments. The increased magnitude of the portfolio dictates a more expansive notion of risk/opportunity diversification. As theater transparency increases the size of data resources from gigabytes to petabytes, similar issues arise. Should commanders use greater information assets to better diversify their campaign strategies & tactics? Or should they use these assets to better focus their initiatives? These are the questions CINCs have to debate.

Arguably the most provocative portfolio management questions might revolve around what information would be least valuable and/or necessary for making critical command decisions. Along what military/civilian dimensions should commanders and their civilian overseers be prepared to actually *reduce* information dependency? The purpose of the portfolio approach is not to create the faux comforts of quantification but to assure that priorities and assumptions are explicitly testable. In global finance, portfolio management is a powerful technique to create a common vocabulary for defining opportunities and risks.

Why? Because the economic questions of how information and analyses should be re-prioritized in an era of growing superabundance have not been adequately answered. Where are the 'Measures of Information/Analytical Effectiveness' - the MOI/AEs - that provide conceptual rigor to discipline the greater volumes of information that technologies enable? These 'prioritization rationales' - whether generated by CINCs or by company commanders - are central to the cost-effective management of net-centric information. Prioritizing in the presence of overwhelming information requires different skills than prioritizing scarcity. More information invariably means more choices and more trade-offs between them.

At this point, a paradox emerges: The more choices you have, the more your values matter. Does doctrine *really* stress casualty prevention and civilian protection? Or does the goal of maximum overwhelming force in the minimum amount of time to achieve policy objectives effectively trump those PCs? When information, computation and analysis become cheap, assumptions become dear. In information rich environments, the data matter less than our assumptions and aspirations.

Operationally, the implications are profound. Better, faster, cheaper and more pervasive information utterly transforms von Moltke's most famous aphorism that, 'All plans evaporate on contact with the enemy.'

Information economics - indeed, the information risk management portfolio - would argue that information superiority makes 'planning' ultimately less valuable than 'responsiveness.' Why? Because, informationally speaking, comparative information advantage accrues *as the rate of information acquisition and analysis changes* over time. The ability to detect and respond to battlespace changes faster, better, cheaper and more pervasively than the opposing force inherently places a premium on better 'improvisation' than better planning. Indeed, the critical combat competency for commanders shifts from rigorous planning - that stochastically evaporates on contact with the enemy - to improvisational responsiveness. The classic example of such improvisational responsiveness was the unplanned, untested role of Special Operations Forces to call in just-in-time air strikes against Taliban forces. (Intriguingly, these improvisations were less 'net-centric' than 'network-enabled'.)

In other words, another 'perverse consequence' of the RMA/net-centric argument is that investing in responsiveness yields disproportionately higher returns than investing in planning. That means that training exercises and experiments should logically focus less on comprehensive plans of attack and more on the ability to flexibly respond to the unanticipated and the unplanned. To be fair, flexibility is enshrined as a core value of the RMA/net-centric/information-based warfare advocates.

Which brings the argument full circle. That technology has transformed - and will continue to transform - military conflict is inarguable. That digital technologies and doctrines will give more soldiers, sailors, airmen and their commanders more information than ever before is inarguable.

But, an honest, unvarnished view of how individuals and institutions actually behave in information rich environments - as opposed to how we might like them to behave - does not assure that greater quantities of data will lead to better quality results. This paper makes the case that there are excellent reasons for this disconnect. The hard work of examining the economics of information - and the perverse consequences that 'information abundance' understandably create - has not yet been done. Capacity is not the same as capability. The National Security community has made enormous investments in providing technical capacity. It has yet to make comparable investments in exploring the economics of how organizations effectively translate that new capacity into new capabilities. That has to change.

## ENDNOTES

<sup>1</sup> Roger Lowenstein, *When Genius Failed: The Rise and Fall of Long-Term Capital Management*, (New York: Random House, 2000)

<sup>2</sup> Theodore Day, Yi Wang, and Yexiao Xu, *Investigating Underperformance by Mutual Fund Portfolios*, (Dallas, TX: School of Management, University of Texas, Dallas, May 2000) also *Global Investor Magazine*, December 2002 (special issue).

<sup>3</sup> Berinato, Scott "What Went Wrong at Cisco?" *CIO Magazine*, August 1, 2001.  
online at: [http://www.cio.com/archive/080101/cisco\\_content.html](http://www.cio.com/archive/080101/cisco_content.html)

<sup>4</sup> Please see Admiral William A. Owens, *Lifting the Fog of War*, (New York: Farrar Straus Giroux, 2000)

<sup>5</sup> Daniel Kahneman and Amos Tversky, eds. *Choices, Values and Frames*, (Cambridge, UK: Cambridge University Press, 2000) and Hersh Shefrin, *Beyond Greed and Fear: Understanding Behavioral Finance and the Psychology of Investing*, (Boston, MA: Harvard Business School Press, 2000)

- <sup>6</sup> Robert R. Leonhard, *Principles of War for the Information Age*, (Novato, CA: Presidio Press 2000) pp. 224-225.
- <sup>7</sup> Ibid, pp. 156-157.
- <sup>8</sup> Charles J. Hitch and Roland N. McKean, *The Economics of Defense in the Nuclear Age*, (New York: Atheneum, 1965) and Alain C. Enthoven and K. Wayne Smith, *How Much is Enough? Shaping the Defense Program 1961-69*, (New York: Harper & Row, 1971)
- <sup>9</sup> Peter Bernstein, *Capital Ideas: the Improbable Origins of Wall Street*, (New York: Free Press, 1992)
- <sup>10</sup> John Maynard Keynes, *The General Theory of Employment, Interest and Money*, (New York: Harcourt, Brace, 1936)
- <sup>11</sup> See, for example Bob Kovach, "US Investigates friendly fire deaths in Afghanistan," *CNN.com*, April 22, 2002 at <http://www.cnn.com/2002/WORLD/asiapcf/central/04/22/ret.friendly.fire/> and *CBC News online*, "Canadian Survivors of friendly fire bombing describe ordeal," January 16, 2003 at <http://www.cbc.ca/stories/2003/01/15/friendlyfire030115>
- <sup>12</sup> See, for example: "Israel divided by policy of target killing," *telegraph.co.uk website*, July 26, 2002 <http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2002/07/26/wmid126.xml> and "A Nation Faces a Bloody Dilemma," *The Age online*, July 27, 2002, <http://www.theage.com.au/articles/2002/07/26/1027497411806.html>
- <sup>13</sup> Frank Partnoy, *Infectious Greed: How Deceit and Risk Corrupted the Financial Markets* (New York: Times Books, 2003) and Mimi Swartz and Sherron Watkins, *Power Failure: The Inside Story of the Collapse of Enron* (Doubleday, 2003)
- <sup>14</sup> See <http://www.wargamesdirectory.com/html/articles/Various/technology.asp> and [http://www.janes.com/defence/news/kosovo/jdw990707\\_01\\_n.shtml](http://www.janes.com/defence/news/kosovo/jdw990707_01_n.shtml) and [http://www.defenselink.mil/news/Oct2001/t10242001\\_t1024dd.html](http://www.defenselink.mil/news/Oct2001/t10242001_t1024dd.html)
- <sup>15</sup> R.V. Jones, *The Wizard War: British Scientific Intelligence, 1939-1945*, (New York: Putnam, 1978) and Robert Buderer, *The Invention That Changed the World: How a Small Group of Radar Pioneers Won the Second World War and Launched a Technological Revolution* (New York: Simon & Schuster, 1996) and Alfred Price, *Instruments of Darkness; The History of Electronic Warfare* (Scribner, 1978) and Alfred Price, *War in the Fourth Dimension: US Electronic Warfare, from the Vietnam War to the Present* (London: Greenhill Books, 2001).
- <sup>16</sup> David MacIsaac, *Strategic Bombing in World War Two: The Story of the United States Strategic Bombing Survey*, (New York: Garland Publishing Co., 1976).
- <sup>17</sup> W. W. Rostow, *Pre-invasion Bombing Strategy: General Eisenhower's Decision of March 25, 1944*, (Austin: University of Texas Press, 1981) and Solly Zuckerman, *From Apes to Warlords - the Autobiography (1904-46) of Solly Zuckerman*, (London: Hamilton, 1978)
- <sup>18</sup> W.J.R. Gardner, *Decoding History : The Battle of the Atlantic and Ultra*, (Annapolis, MD: United States Naval Institute, 2000) and Kenneth Macksey, *Without Enigma: The Ultra & Fellgiebel Riddles*, (Surrey, UK: Ian Allan, 2001)
- <sup>19</sup> Montgomery C. Meigs, *Slide Rules and Submarines: American Scientists and Subsurface Warfare in World War 2*, (Washington, DC: National Defense University Press, 1990)
- <sup>20</sup> Ralph Bennett, *Intelligence Investigations: How Ultra Changed History*, (London: Frank Cass, 1996).
- <sup>21</sup> General Wesley K. Clark, *Waging Modern War: Bosnia, Kosovo and the Future of Combat*, (New York: Public Affairs, 2001)
- <sup>22</sup> Barton Gellman and Thomas E. Ricks, "US Concludes Bin Laden Escaped at Tora Bora Fight," *Washington Post*, April 17, 2001, p. A01 online: <http://www.washingtonpost.com/ac2/wp-dyn/A62618-2002Apr16?language=printer>
- <sup>23</sup> PMS Blackett, *Studies of War, Nuclear and Conventional*, (New York: Hill and Wang, 1962)

## SUGGESTED READINGS

Belsky, Gary and Thomas Gilovich. *Why Smart People Make Big Money Mistakes and How to Correct Them.* (New York: Simon&Schuster, 1999)

Hartcup, Guy. *The Origins and Development of Operational Research in the Royal Air Force.* (HMSO, 1963)

Jorion, Phillippe. *Value at Risk: The New Benchmark for Managing Financial Risk.* (New York: McGraw-Hill, 1999).

Miller, Ross. M. *Paving Wall Street: Experimental Economics and the Quest for the Perfect Market.* (New York: Wiley, 2002).

Mirowski, Philip. *Machine Dreams: Economics Becomes a Cyborg Science.* (Cambridge, UK: Cambridge University Press, 2002).

Savage, Sam. *Decision Making with Insight.* (Wadsworth Publishing, 2003).

Taleb, Nasim. *Foiled by Randomness: The Hidden Role of Chance in the Markets and in Life.* (New York: Texere, 2001).

Thiesmayer, Lincoln and John Burchard. *Combat Scientists.* (Atlantic Monthly Press, 1946).

Wilmott, Paul. *Paul Wilmott Introduces Quantitative Finance.* (New York: Wiley, 2001).

Wilson, Andrew. *War Gaming.* (Pelican Books, 1970).