The TECHNOLOGY Trap

U.S. NAVY (INEZ LAWSON)

John Kruse, PhD & Mark Adkins, PhD

The military invests heavily in technology, often ignoring its impact on the users, assuming that "If we build it, they will come." Carrier Group 3 proved the importance of the human element in network-centric operations.

On 12 September 2001, the Carrier Group 3 staff on board the USS *Carl Vinson* (CVN-70) arrived in the North Arabian Sea. The staff had originally prepared for a routine Southern Watch deployment but the tragedy of 9/11 abruptly changed the mission. As the U.S. 5th Fleet's Commander Task Force 50 (CTF-50), they instead led a coalition force of 59 ships in combat operations against Afghanistan during Operation Enduring Freedom, and demonstrated the most successful grasp of network-centric operations yet witnessed above the tactical level.

Foundations of Collaboration

Humans are born collaborators. We are social animals and almost every worthwhile development or achievement is the result of group effort. Organized warfare is no different.

Trust has always been a key issue intertwined with collaboration. People in general, and warfighters in particular, build strong bonds with their comrades. Military leaders place a high priority on building unit cohesion, chiefly because there is a tacit understanding that these bonds stimulate people to willingly work beyond expectation, even in mortal danger.

At the lowest levels, our forces organize primarily through deconfliction. Because of limitations on the currency and accuracy of information, warfighters cannot be expected to understand what is happening beyond their own small slice of the battlefield. As a result, planners use assigned altitudes, controlled fire lines, synchronization matrices and unit boundaries, to deconstruct the battlespace into manageable chunks. This approach maximizes task specialization, but fails to tap into potential synergies.

Deconfliction's primary casualties are efficiency and effectiveness; it is an inherently rigid system that does not allow for rapid or flexible responses. One commonly finds on such battlefields some units over-committed while others have little to do. Moreover, change becomes difficult once the rules for deconfliction have been instituted.

Network-centric operations, on the other hand, permit speed, initiative, and independent action. The concept allows units to maximize their own effectiveness. Rather than waiting for direction, commanders are free to act on their own initiative in support of the command intent. This permits commanders to engage the enemy more often, for greater duration, and in novel ways.

The Lure and Acceptance of Technology

Some World War II-era Pacific islanders, particularly in New Guinea, were amazed by the great wealth that arrived with the war effort and came to believe that it was the newly constructed airstrips and harbor facilities that attracted the planes and ships. Failing to realize that trade infrastructure was a necessary—but insufficient—condition for bringing a tide of goods, what came to be known as "cargo cults" cleared airfields, built wharves, lit signal fires, and sat in rudimentary control towers waiting in vain for the bounty to arrive. In much the same way the Department of Defense is spending billions of dollars constructing complex interwoven technologies, all the while making the assumption that collaboration will just happen once the infrastructure is built. There has been a flurry of planning, spending, development, and fielding. Unfortunately, much of this expense and effort is focused solely on technology and, while necessary, technology alone is an insufficient precondition for effective network-centric operations.

What is missing is a simple and clear understanding of how and why people adopt technology, ingrain the tools in everyday work, and use the systems to collaborate effectively. Without a simple model of human behavior, technologists and leaders are independently deciding how best to advance network-centric operations. The study of CTF-50 helped to refine and cement our views on how the military can break out of the "build it and they will come" mentality to exploit the capabilities of network-centric operations.

Successful adoption of new technologies is based on two primary factors: (1) Aggregated net value—the benefit expected each time a technology is used combined with the frequency of anticipated technology use, and (2) perceived complexity—the effort associated with using the technology.

A relatively uncomplicated and frequently used technology like e-mail is easily adopted as users realize significant value on a daily basis. A technology with less benefit and/or low frequency of use may not be able to overcome its perceived complexity to achieve a successful adoption. Although tax software, for example, may be quite easy to use, one may not be willing to put forth the effort to realize a benefit that accrues only once per year. On the other hand, a user may be willing to take on a fairly complex technology if the perceived rewards are evident. People are not willing to expend resources if they do not expect to gain significant return on the investment.

An obvious key to assuring technology adoption is to follow the time-honored KISS maxim—Keep It Simple, Stupid—while still delivering value to users. A second building block for technology adoption success, however, high frequency of use, often goes unrecognized. This is surprising in military environments as this principle is tacitly acknowledged in the oft quoted saying that you should train the way you fight. A gun or aircraft crew will drill frequently, eventually making system operations second nature. Rarely is such effort applied to network-centric systems training.

Too much attention is being paid to the technical facets of NCO development to the detriment of the important human aspects.

Building a Trusted Network

CTF-50's leadership avoided many technology pitfalls and fleshed out network-centric operations capabilities through several approaches. First, the leadership designated specific technologies as collaboration standards: (1) voice circuits for immediate threats and orders; (2) electronic chat for time sensitive information and administration; (3) *CommandNet* collaborative logs to create chronological records of critical events; and (4) *Knowledge Web (KWeb)* to provide analyses and detailed information in web pages. All staff briefings were given directly from existing *KWeb* pages with support from chat and *CommandNet* collaborative logs. PowerPoint was never used once. Second, the CTF-50 commander deemphasized competing technologies. Staff members curtailed record message traffic and directed outside entities and higher

U.S. NAVY (RICHARD R WAITE)

Operations Specialists 3rd Class Joseph Quintana (left), Sara Hacket (center), and Operations Specialist 2nd Class Ryan Archer monitor Global Command Control Systems in the Combat Direction Center on board the USS John C. Stennis *(CVN-74). Network-centric operations allows access to information that had been narrowly distributed in the past, making it readily available during ad hoc tactical or operational discussions.*

commands to access the *KWeb* pages. Finally, the CTF-50 leadership made a concerted effort to reward information sharing and innovation.

Implementing the three command initiatives increased the value of using the systems and the frequency of use throughout the fleet. Information contributors and consumers alike received benefits when current and accurate information was posted to *KWeb*. In time, even the resistant users in CTF-50 came to view the network-centric operations capabilities as indispensable.

Network Effects

Before the advent of network-centric operations at Carrier Group 3, information distribution was challenging; formats, media, and transmission of information were unwieldy and inefficient. Network-centric operations capabilities significantly lowered the barriers to sharing information. Staff members simply put the work required to develop PowerPoint shows into maintaining accurate web pages. Because these pages were automatically shared, the staff as a whole became better informed and more responsive. Both internal and external consumers now had access to information that had been narrowly distributed in the past. Watchstanders were even studying the *KWeb* out of curiosity and a desire to understand the operation.

Over time, other important network benefits were found. Although not immediately realized by the staff, the development of trust had changed. Prior to NCO capabilities, relationships developed through personal networks; now people were creating close working ties through chat and monitoring *KWeb* pages. The constantly updated information allowed widely distributed users to feel informed and connected. The measure of success among the staff became a useful and current *KWeb* page. In effect, the staff found that one could trust a person who was diligent in publishing quality information. CTF-50's commander reinforced this new means for gaining status by giving public recognition to the best information providers. At first, the concern was that people would hoard information; the opposite was true and staff members were actually competing to share more and better information.

Originally, staff members feared that the new technologies would just add work. Instead, duplication of effort was eliminated and people were freed to work more efficiently. The commander made a point that he did not expect perfection on the network. The leadership was aware that a common mistake of staff members is to play it safe and be overly conservative. He told everyone that he wanted people to give their best information estimates on the network and that no one would "get their head cut off" for making a mistake. He allowed draft documents and gave petty officers the authority to publish on their own without vetting their work through superiors.

As the *KWeb* became established in the task force, this streamlining effort paid off handsomely. The staff made battle plans with more accurate, rather than more cautious, estimates. *KWeb* pages were accessible in staterooms and duty stations, making accurate, timely information immediately available during ad hoc tactical or operational discussions. The command made it safe, even desirable, to

be both an information provider and consumer. Eventually, this gave rise to some long overdue social changes.

Cultural Shifts

The United States Navy, like the other services, is filled with dedicated people, but sometimes a good thing can be taken too far. Overzealousness can impair effectiveness. Automation efforts within CTF-50 allowed the command to chip away at some of the command's more dubious norms.

The admiral set the tone by urging staff members to sleep and have time to wind down without guilt. Because the staff members would update systems throughout the day, they were not tied so strongly to an inflexible schedule. To drive home the message, the CTF-50 commander publicly played cards almost every night. By seeing regular recreation among senior officers, the staff felt free to do the same when work loads permitted. Senior leader interviews revealed that this enabled the staff to more easily shift gears when true emergencies surfaced.

There were even gains realized outside of the task force. Normally a strike group staff spends a great deal of time responding to information requests from fleet and theater commands. The CTF-50 staff had direct orders to avoid tracking down information requests. Instead, they directed the requestors to the appropriate *KWeb* page. The admiral stated, "We were in the middle of a war, and we weren't getting any calls (from higher headquarters)" because of *KWeb* and *CommandNet*.

Security is a prospective problem that is often associated with network-centric operations information sharing. By lowering the barriers to gaining information, the force also opens up new opportunities for those that might breach the system either on purpose or inadvertently. A wealth of information was available on the NCO systems to anyone with classified internet access. Network-centric operations theory dictates that information should be readily available. This high degree of freedom does, however, require greater responsibility and discretion on the part of information producers and consumers in the absence of other checks and balances. CTF-50 generally found that the potential hazards far outweighed the benefits.

Associated with the security issue is that of visibility. CTF-50 took significant risks by opening up the command to outside scrutiny. One visiting U.S. Air Force general was shocked that he was able to drill down into the *KWeb* and find detailed weapons status information. He expressed a common fear that such transparency would enable 5th Fleet and Central Command the ability to micromanage the task force. Instead, CTF-50 found the greater levels of information made the higher commands more trusting. This reinforced the commander's mantra, "A smarter, more informed boss makes life a whole lot easier."

Lessons Learned

In the end, the CTF-50 staff leveraged simple, general-purpose technologies to radically change the way they prosecuted the war. This was no small feat as they were obliged to drastically ramp up the size of the fleet, work closely with coalition members, and shift focus to an unanticipated mission. This look at CTF-50 was surprising, as it identified the extent to which social and cultural factors governed the transformation. The initiative succeeded in large part due to the leadership's willingness to allow people to self-synchronize in the context of the trusted virtual team.

This case study research identified six general lessons that, if adopted, will help leaders move their organizations towards a successful transition to network-centric operations.

Lesson #1: Systems that provide value up and down the chain of command get used.

Recommendation: Field systems that benefit more than just the boss.

Lesson #2: Inexpensive and simple technologies can be very effective if a common structure is enforced.

Recommendation: Put less emphasis on building specialized "holy grail" systems and field available, general-purpose ones now.

Lesson #3: Frequency of use is key to both adoption of tools and establishing virtual communities of trust.

Recommendation: Select systems that require regular interaction and involvement from contributors and consumers.

Lesson #4: Network-centric operations shouldn't create more work.

Recommendation: Emphasize the desired communication channels and stop duplications of effort.

Lesson #5: Engaged people will innovate.

Recommendation: Let people experiment – experienced users expand system use and derive more value.

Lesson #6: Waiting for perfection has costs.

Recommendation: "Just do it" - Take calculated risks, a best guess today is often better than a perfect answer next week.

This research was initiated with the expectation of finding operational improvements resulting from network-centric innovations at CTF-50. However, we did not expect to discover all of the social domain preconditions and benefits associated with the transformation. Too much attention is being paid to the technical facets of NCO development to the detriment of the important human aspects. Unless leadership, training, development, and acquisition of network-centric operations capabilities are coordinated, there is the risk of becoming a technology cargo cult that builds networks in a vain attempt to spawn collaboration.

Dr. Kruse is the Director of Systems Development at the University of Arizona's Center for the Management of Information and has worked extensively with the government and military to develop group processes and software to support collaborative work. Dr. Adkins is the Director of Research at the University of Arizona's Center for the Management of Information. He has worked extensively with COMTHIRDFLT to develop group processes, improve decision-making, and build collaborative decision spaces.