

SIGNAL ONLINE

More than a magazine: We're AFCEA.

The Vulnerability of Technology

By Rear Adm. Hamlin Tallent, USN (Ret.), and Capt. Thomas H. Lang, USN (Ret.)

July 15, 2011

The U.S. Navy may be setting itself up for strategic mismatches of historic proportions in the near future. While its perception of victory may be tainted by the vision of several aircraft carriers of the Imperial Japanese Fleet listing heavily, on fire and dead in the water during the Battle of Midway, today's mismatch could likely center on the expectation of data flow in the face of an adversary's ability to deny it.

Past victories represent the very visceral type of kinetic outcomes that practitioners of the western way of war prefer when forced into conflict. But what if victory in future wars does not look anything like that? What if there is no kinetic component at all—no explosions, no debris, no wreckage and no bodies? In certain situations, victory in future conflicts might simply look like no war has been fought at all. The only trace might be the image of a U.S. carrier task force that suddenly turns around and returns to home port. The interruption of critical command and control data streams could cause such an outcome when inflicted on a force that has come to rely too heavily on those streams of ones and zeroes.

Since the late 1980s, the Navy fleet inventory has declined

from nearly 600 ships to less than 300. The thinking has been that the sophisticated technologies that power today's command, control, communications, computers, intelligence, surveillance and reconnaissance (C⁴ISR) enable a full range of functions to be carried out by fewer ships and with fewer people.

In addition, the widespread adoption of faster, more capable data handling and information processing tools has been the ubiquitous incorporation of those capabilities into a wide variety of situational updates provided to senior leadership. Briefings are often seen as proving grounds where more complex, animated slides are used to display snapshots and video clips that convey ever more complex ideas to an audience. The result of this evolution is an audience that has become a far more sophisticated consumer of data than in previous years.

However, with that sophistication has come a certain amount of reliance on such data and a mistaken notion that vast quantities of disparate data—and the systems needed to process them in real time—are absolutely critical to effective execution of the command and control process. Such beliefs in the nearly sacrosanct nature of some data

streams and information processing capabilities open up U.S. forces to a broad range of vulnerabilities that did not exist in years past. Those vulnerabilities provide our enemies with a whole host of lucrative targets.

Consider the challenges to a maritime Joint Task Force or battle group commander if significant pieces of command and control capabilities were lost during operations. The confusion would be immediate and wide-ranging. It would include trying to organize teams to undertake the denial and to determine the indicators and causes, who assesses the effects of denial on the plans in operation and who decides to go to alternative plans as well as the rules of engagement. In addition, what if that same commander is denied the infrastructure needed to enable forward-deployed units to continue executing functions of the plan without real-time situational awareness and pass orders? The reality is that in some if not most cases, degradation of portions of existing C⁴ISR portfolios will force operations to suspend and result in defeat without a shot fired.

Regardless of how much planning occurs, the ability to advance via alternative means is crucial. The answer will lie in

the ability to break down plans into isolated, discrete, critical acts and to determine if and how the military can conduct those acts with degrading or nominal support. For instance, a plan might call for placing a bomb on a crucial aim point. A minimal C⁴ISR construct would be to use a manned aircraft with an internal delivery capability such as a laser-guided bomb instead of a SATCOM-tethered unmanned aerial vehicle using Global Positioning System technology.

To execute this solution will require some work. Military leaders must have the ability to plan within a degraded C⁴ISR

environment and to organize a competent team that can identify the nature of the C⁴ISR degradation and potential mitigation strategies. They must be able to develop the skills necessary to identify the technological threats to on-going planning and execution efforts rapidly. They also must be able to evaluate the severity of those threats as well as the ability to construct and pass orders that are detailed enough to execute in the absence of constant direction. Finally, they need the willingness to command in the absence of near-perfect situational awareness and to train for this degraded environment at the

unit, intermediate and advanced levels during pre-deployment training evolutions.

It may be time for the Navy to take an enterprise approach to solving this potential strategic mismatch and thoroughly explore the nature of future conflicts, not just automatically project an ever more technological set of challenges and solutions. It may be time for the Navy to re-read and understand the words of Clarence Darrow: "It is not the strongest of the species that survives, nor the most intelligent, but the one most adaptable to change."

Rear Adm. Hamlin Tallent, USN (Ret.), is the vice president of C⁴ISR systems at Sentek Global. The retired flag officer served as director of operations for the U.S. European Command. Capt. Thomas H. Lang, USN (Ret.), is a program manager at Sentek. While on duty, he served as the senior intelligence officer for the Naval Special Warfare Command and in a similar billet for the U.S. Third Fleet.