

The What Where and When of Making Net-centric Warfare Real Today

Rich Byrne, The MITRE Corporation

Recent successes in Afghanistan and Iraq introduced the world to a new military paradigm. Joint operations, information superiority, and bringing to bear the power of the full military network to every fight are touted as evidence that we are achieving net-centric warfare. However, in reality we are just in the infancy of this revolutionary shift in capabilities. In the battlefield, we have islands of stove-piped communications that can only pass information between the same types of equipment and fail when dissimilar systems need to exchange critical information. Far too often each system has its own data format that is complex and non-interoperable with other systems without slow and error prone, human-intensive translations. Many believe we must accelerate the massive planned DoD investments to recapitalize both our communication networks and our data systems before we can truly benefit from the promises of machine-to-machine net-centric warfare. Unfortunately, such investments will take at least a decade to become commonplace in the battlefield.

In the meantime, is there anything we can do today? The answer is a resounding yes if we simplify our focus to just the most important information that needs to be shared. A tourist in a foreign country can function quite acceptably by only learning a small number of key words. These key words generally are the same regardless of which foreign country is being visited. Our military systems are each like a different foreign country trying to learn the full languages and cultures of every other system they need to speak with. No wonder this is too expensive and complex to accomplish. If, on the other hand, we can identify a handful of words that are absolutely the most important, we can teach each system how to translate those few words from their 'native' language into a common 'esperanto' language. We choose a common language so every system only requires one translator (not one for every other native language that it needs to work with). Now each system not only learns just one common language, but only a few words in it. The cost and complexity have been so greatly reduced that this can be accomplished today for any system in weeks not years.

So what are the magic words for a net-centric battlefield? After an analysis of what goes on in modern battles, we have found that "What", "Where", and "When" constitute the most valuable information for an amazingly large number of the most critical missions that need to exchange information across many systems. "What" tells us if this is a friendly or hostile force; a target to be killed or a survivor to be rescued. "Where" has become synonymous with military GPS accuracy of precision coordinates that guide munitions

through windows or navigate tanks through zero visibility sandstorms. "When" is becoming increasingly important as we dramatically shrink the sensor-to-shooter timeline for "time-sensitive-targeting" missions.

As evidence of the potential, several initiatives have been undertaken by the Air Force and MITRE to rapidly deploy just such an information strategy to a number of fielded systems. A common "What", "Where", and "When" standard is used, enabling any system that learns those few 'words' to exchange this data with any other system that makes the same modest investment. The software required is modest indeed (a few hundred to a few thousand lines of code); it can be readily added to existing fielded equipment (no new hardware) and it is compact enough to run across even the oldest radio links and networks being used (no need to wait for new systems to become net-centric). Machine-to-machine information exchanges are then easily automated (no more slow, error-prone human translations) with humans only in the loop for the key decision making steps. How is it used? First, precision targeting information is shared between systems that could only do so before via voice transmission, human transcription, and manual data re-entry. Next, friendly locations are shared from the set of blue force tracking systems to systems that previously couldn't receive it—reducing the probability of fratricide. This strategy can be applied to a number of intelligence, surveillance, and reconnaissance (ISR) information flows, such as those from unmanned air vehicles (UAVs) to enable the warfighter to get ISR information "on demand". The AF/MITRE work has drawn inquiries from dozens more systems regarding how they can add their universal What, Where, and When capability. The grass roots approach has been very successful but has its limits, particularly when it comes to fielding across the enterprise. Is it time for the DoD to encourage the adoption of a *common, small* set of the *most important* information across all battle systems, to provide technical support to illuminate the power of this approach, and to offer assistance in its implementation? Since much of the value of net-centric warfare can be quickly achieved for little cost, we believe the answer is yes.

This is not to say that longer-term activity isn't also needed to realize the full potential of net-centric warfare. Robustness, information management, and information assurance are examples of areas needing more attention. Nevertheless, the DoD should seize the opportunity today to rapidly tie systems together using the What, Where, and When approach.