

CRITICAL FACTORS AFFECTING THE MILITARY UTILITY OF NETWORKING

Alfred Kaufman¹

Abstract. This article is a first cut at quantitatively exploring the conditions under which the fundamental tenets of the Network Centric Warfare doctrine might be valid. It is based on a somewhat more extensive study of the subject published by the author [1] and covers three related topics: the situational awareness that is made possible by networking of battlefield sensors, the onset of cohesive behaviour amongst the human actors involved in operating networked systems, and the limits of human proficiency. The paper shows that the situational awareness obtained through the network is not automatically better than that obtained from individual sensors and identifies the conditions under which it might be; it shows how the cohesive behaviour is increased by the size of the networked community, by the quality of leadership controlling that community, and by the degree of individual proficiency with which members join the community; and it shows how recruiting, training, retention, and the quality of life will affect that individual proficiency. In the end, the article summarizes the various factors which must be addressed before the promise of networking can be realized.

A great deal has been said recently about the benefits of networking a military force, but all of what has been said is largely qualitative and always hypothetical; one would be hard put to find any quantification of the supposed military utility of a net-centric way of war. In this article I will take the first step down this un-travelled path.

Like all travel in uncharted territory, my journey will be exploratory rather than exhaustive. Instead of trying to prematurely construct a detailed model of the military utility of networking, I will strive to identify those factors which control the degree of the utility realistically achievable in combat and provide just enough quantification to be able to judge which of them are likely to drive combat benefits.

Networking of military systems is expected to produce performance synergy, otherwise one would not bother to do it. This networked-enabled synergy can manifest itself in two different ways: an increase in system performance resulting from the data exchange with other like systems that is made possible by networking, and an increase in human performance resulting from the onset of a cohesive behaviour among the human actors involved in the operation of these systems made possible by communication through the network.

DATA EXCHANGE: GAINING SITUATIONAL AWARENESS

Imagine we wish to gain an understanding of what happens on the battlefield. This information is usually obtained through the deployment of various sensor systems able to collect data about the enemy and the lay of his forces. The data collected by a sensor is a stochastic process from which the system processor generates a certain statistic characteristic to the sensor employed. That statistic is then compared to a predetermined threshold and if the statistic exceeds that threshold, the battlefield feature under observation is said to be present. Otherwise the feature is said to be absent. Although the process of gaining situational awareness would probably have to include identification and classification of the detected object in addition to mere detection, we shall only consider the simplest of all cases when detection was enough.

Because data collected by the sensor is of necessity stochastic in nature, there is only a certain probability that the information thus collected about the presence of the battlefield feature under consideration corresponds to reality.

This implies that there is also a certain probability that the information does not. These two probabilities are the sensor's probability of detection and the sensor's probability of false alarm, respectively. Specifically, the probability of detection measures the probability that the sensing system will ascertain the presence of some feature in the battlefield when that feature is actually present. The corresponding probability of false alarm measures the probability that the sensing system will ascertain the presence of that feature when the feature is not, in fact, present. These two probabilities represent performance characteristics of the sensor under consideration and depend both on the sensor's construction as well as on the tactical and environmental circumstances under which it is employed.

When we join a set of such sensors into a network in which they are allowed to freely exchange data with each other, the network manager is possessed by a collection of stochastic bits of information each of which is provided to him by a sensor in the network. From this collection, he develops situational awareness about the battlefield. The situational awareness he builds out of these bits of information is therefore equally stochastic in character. Consequently, there exists only a certain probability that his surmise about the battlefield corresponds to the real situation on the ground. Clearly, unless that probability is larger than the corresponding probability resulting from the sensors alone, networking will have proved to be of very little value. We should therefore explore the conditions under which the probability that the manager's surmise is correct exceeds the corresponding probability as provided by each sensor in isolation.

To accomplish this goal, we need to first quantify the process by which a network manager develops his situational awareness. Since the bits of information provided by the various sensors about any given feature in the battlefield need not agree with each other, a network manager must develop a set of rules for brokering between the sensors. A reasonable, though not necessarily practicable, way to do that would be to combine the information provided to him by all the sensors using a Bayesian statistical-inference technique. Specifically, imagine that $p(YES)$ represents the prior knowledge available to the network manager concerning the presence of a given feature in the battlefield, and let there be a sensor employed to observe that feature. According to Bayes' law, the state of knowledge available to the manager after the sensor has made

¹ Institute for Defense Analyses, 4850 Mark Center Drive, Alexandria, VA 22311-1882, USA.