Network-Centric Warfare

An Approach to 21st Century Warfare

by

Mark R. Kellenberger

IST 210, Section 50
Professor Konak
April 28, 2005
1. The Philosophy of Network Centric Warfare

The success of our military’s most recent conflicts in Afghanistan and Iraq have come out of a modern warfare strategy that uses networking concepts to create an “informed force”. The concept of Network Centric Warfare is the central theses of a larger plan called Transformation that has been reshaping the military since the 1990’s. Transformation was put on a fast track after the events of September 11th, 2001 as our nation was propelled into a new global paradigm on defense. While Network Centric Warfare is still in its infancy, it stands to potentially make as big a change to war fighting as did the advent of gunpowder. War is fought by man, and will continue to be fought by man, but the military has begun to transition to an information philosophy that revolves around highly sophisticated technology to gather, disseminate and utilize information to fight. The philosophy and the hardware allow combat troops to improvise on a plan, increasing their efficiency and lethality. Network Centric Warfare differs from 20th century warfare in that information is not held by the top echelons of command. Information is cleared out to tactical personnel allowing them to operate as linked groups. Informed forces make better, quicker decisions. If your side has better information on the operation, you have the advantage of shaping the battle to your strengths thereby enhancing your chances for success. Transformation relies heavily on technology and two pieces of that technology are the Interim Armored Vehicle and the Unmanned Aerial Vehicle. The ability of these vehicles to gather and disseminate information in the networked war is unprecedented in warfare.

2. Hardware Used in Network Centric Warfare

The modern battlefield depends on linked units to project power. In the Iraq situation, there are naval units at sea linked with combat and surveillance aircraft over the theatre, the air units in turn, are linked to units on the ground. Everyone is connected creating the information battlespace. At the tactical level, the Army is deploying a new vehicle to act as a ground node in the network. The Interim Armored Vehicle (IAV), known as the “Stryker”, is a 19-ton vehicle that can be outfitted to serve a variety of purposes. The IAV is deemed “Internetted” as it contains a communications package broadly known as C4ISR. This acronym, C4ISR, stands for command, control, communications, computers, intelligence, surveillance, and reconnaissance. While many of the mobile units the Army has deployed are “Internetted”, the Stryker is unique
in that it’s been designed to fight the network centric war. NOVA recently ran a special titled, “Battle Plan Under Fire”, displaying the power this machine has as an information gathering appliance. With a full squad on board, the Stryker deploys its personnel armed with night vision goggles and communications links to discover information. The Stryker will then use the information and disseminate it throughout the command and control structure. The specifications are impressive. According the Armed Forces Communications and Electronics Association, the C4ISR Architecture gives it a Super High Frequency (SHF) uplink to a military satellite sending tactical data and secured voice transmissions. The Stryker can communicate locally via communications and data links to in-theatre units as well as ultra-high frequency (UHF) satellite communications for regional communications. The computer software is a UNIX based system running on battle ready computer systems (author’s note: the nomenclatures are so cumbersome the reader is directed to the references). All units are equipped with global positioning system (GPS) receivers for navigation. The most remarkable result of all of this connectivity is “Blue Force Tracking”. The Global Positioning System in concert with the satellite link allows for tracking of the vehicle via satellite. The combined view gives all commanders an unprecedented view of the battlespace as friendly units can be marked with their corresponding position and heading. The vehicle itself is somewhat of a hub that links individual ground units together. The networking possibilities are endless because as units engage enemy forces, that information can be updated informing the force so that they know how to react. Because the system is inherently redundant, disabling a Stryker does not stop the data coming in from the field. Other units in the fight will be sending similar data giving a fairly reliable picture of the action (combat is rather chaotic). Stryker units are not limited by weather, terrain or adversary and once engaged, they can deliver an array of ordinance from small arms to 120mm mortars. These units create the most lethal ad-hoc network in the world today when they are operating on the battlefield. Another of the “wonder” weapons is the unmanned aerial vehicle and the capability it is bringing to the battlefield.

Another story from “Battle Plan Under Fire” recounts the tales of an unfortunate convoy of Taliban and Al Qaeda traveling to a Mosque outside Kandahar. It is evening and they are being watched closely from a Predator unmanned aerial vehicle. The Predator eventually directs and AC-130 Specter Gunship in on the targets destroying the convoy while leaving the Mosque unscathed. Three amazing pieces of technology were at work in this operation: the predator
unmanned aerial vehicle, Synthetic Aperture Radar, and Precision Guided munitions representing the cutting edge in the airborne wing of Network Centric Warfare.

The predator represents the absolute frontline of technology on the battlefield. At $4.5 million a copy, this drone makes it incredibly difficult to carry on operation while it is in the sky. The Predator can loiter around an operations area at an altitude of 25,000 feet for up to 16 hours. Coupled with the fact that it is 27 feet in length with a 50ft. wingspan, it is almost impossible to spot. The technology inside a predator allows for seeing and sending its information. The Predator has high resolution color cameras for daytime operations, infrared for night vision, and radar known as synthetic aperture radar. The synthetic aperture radar is a technology devised by NASA that was originally used to map the surface of Venus. Synthetic aperture radar specially processes the return it receives to develop a grayscale image of the ground below in any weather-day or night. The images give enough detail to identify structures. Figure 1 is a synthetic aperture radar image of Washington D.C. during a snowstorm! Predators also take “wireless” networking to the extreme. The predator is flown by a technician in a remote area away from the battlefield. During the conflict in Afghanistan, Predators were remotely piloted from the country Kyrgyzstan 600 miles from the combat zone. Once over the desired area, the Predator can begin sending its data up the same satellite networks the Strykers are hooked into adding another source of information to the picture. The biggest advantages to the Predator is that it is a bargain compared to what goes into putting an aircraft in the same role. The costs of putting a manned vehicle at the same point just doesn’t compare. Predators have increased in use and have been outfitted with missiles to actively engage targets it finds. Other vehicles are in the pipeline but have not proven to be as versatile as the Predator. The final piece of the network is the projection of power to the enemy. There are many high technology weapons but none have been more useful than the Joint Direct Attack Munition (JDAM).

The JDAM is actually a kit that converts bombs into a precision munition. The kit consists of a tail section that contains an Inertial Navigation System/Global Positioning System. The bomb is given the coordinates of where it is supposed to land from the plane it is connected to. Once deployed, the weapon will continue to be corrected down to the target. The bomb is “dead-on” with a listed error of as little as 13 meters (43 feet) under the best conditions and 30
meters (95 feet) under the worst.\textsuperscript{6} In “Battle Plan Under Fire”, Michael Vickers a former member of the CIA Special Operations Forces and the current Director of Strategic Studies, Center for Strategic and Budgetary Assessments, states that in the first Gulf War about 7 percent of the ordinance dropped was precision guided. These munitions were also incapable of being used in all-weather scenarios since they required a laser beam to illuminate the target. The modern JDAM, with GPS capability, is not limited by weather or any other battlefield conditions.\textsuperscript{10} By networking all levels of the force, including the weapons, we are developing tactics the enemy just simply can’t use.

3. HOW IS IT USED?

The weapons are just part of the bigger war-making policy of the military. Command and control has changed with all of the networked units giving commanders ability never seen. Consider that the United States invaded France in June of 1944. It took 11 months to defeat the German Army. It took 21 days to conquer Iraq. Part of the success was the increased tempo of operations from Network Centric Warfare. When you can see all of your units via Blue Force Tracking, see the enemy via unmanned aerial vehicles you are now in a position to place your forces in the field at the point where their effect will be maximized. In an interview titled “Transforming Warfare”, Admiral Arthur Cebrowski Director of Force Transformation at the Department of Defense compares Network Centric Warfare to 20\textsuperscript{th} century war-fighting. In the industrial age, the least connected people in the chain of command were the ones most in harm’s way. The strategy was to then mass troops, thus imprecise warfare. Physical force (massed artillery, strategic bombing, nuclear weapons etc.) was how an enemy was defeated. The “Physical Domain” dominated warfare. The “Information Domain” provided mostly information to the top tiers of the command structure and proved secondary to physical force. In network Centric Warfare, the two domains still exist but the information domain has increased in both its scope and value. Networking units increases the rate information moves increasing its value. Knowing where a bad guy is eliminates the need to destroy the whole village. So by increasing information flow you have to decrease the need for physical force. The force has become informed creating a “Precision Force” domain. What of Command? Well, Admiral Cebrowski defines yet a 3\textsuperscript{rd} domain; the “Cognitive Domain”, that deals with combat knowledge. When the
Information Domain and the Cognitive Domain merge we see new tactical plans and procedures for conducting operations. It may seem obvious, but a networked force is an informed force and an informed force has the edge of knowledge. It doesn’t always dictate the outcome but according to Admiral Cebrowski in just about every measure, the networked force outperforms the non-networked force because they can do things tactically the enemy cannot do.

4. Disadvantages

The question is a simple one. How do you avoid infrared imaging, spy satellites, unmanned aerial vehicles and the like? To most people the answer would be hiding! In Afghanistan (Tora Bora Mountains) and in Iraq (Fallujah, Ramadi, and Baghdad) our opposition has done exactly that. To be seen is to be killed thus avoid being seen. Technology is negated when the enemy is hiding. It comes down to a good old-fashioned fight between men at this level and here is where we as a military will always be matched. In an article aptly named “The Immutable Nature of War”, Lt. General Paul Van Riper states exactly these facts about warfare. General Van Riper’s criticisms of Network Centric Warfare are not unfounded. In a $250 million war game dubbed “Millennium Challenge” General Van Riper was chosen to lead the “Red” team in this very expensive game. By the fourth day, he had destroyed 16 “Blue” force ships and had forced the games to be reset. General Van Riper’s criticism is totally valid and helps to explain the insurgency in Iraq well. General Riper believes that Network Centric Warfare places the science in front of the art. His chief complaint is that the policy wing of the Department of Defense is removing the thinking out of the art of war. He feels that America is blindly subscribing to the doctrine of Network Centric Warfare without looking at the “immutable nature of war”. He has some facts to back his argument up. In the Millennium Challenge war-game, his feeling was that Blue assumed control because they had the “policy of pre-emption” guiding them. He knew they wanted a fight and rather than wait for them to “pre-empt”, he used a little pre-emption of his own. General Van Riper then concluded that if they were going to strike why wait? Then turned and attacked them. The second example is the Iraqi insurgency. He feels that since there was no definitive conclusion to the Iraq conflict, the enemy has no feeling of defeat. With no figure of authority signing a surrender document with the coalition, coupled with what he believes were not adequate troop levels in theatre, you get the current state of affairs. In a sense, General Van Riper’s thoughts are interesting about Network Centric Warfare: “What I see
are slogans masquerading as ideas. In a sense, they make war more antiseptic. They make it more like a machine. They don't understand it's a terrible, uncertain, chaotic, bloody business. So they can lead us the wrong way. They can cause people not to understand this terrible, terrible phenomenon”.

5. The Future of Network Centric Warfare

Network Centric Warfare is in its infancy. Compare it to business systems and you see that they have only begun to reach a practical level. The future of networked warfare will see several important changes. The first is the increased rate at which information will go from sensor to user. Information will move at faster rates allowing for a more precise force to be applied. Second is the evolution of combat tactics employing the force; our troops will just get better and better. Third is that war will still entail the destruction of life and property as that is, as General Van Riper says “immutable”. The misgivings of Network Centric Warfare are the politics involved with any government action. Will our future leaders be able to support such rapid operations with equally robust foreign policy initiatives? One can see that the current state in Iraq is due mainly to an unstable political situation. Optimistically, if you view the domains that Admiral Cebrowski talks about you see the non-lethal domains increasing and the physical domains decreasing. Maybe, just maybe, networking will solve man’s desires to kill his fellow man.
Works Cited


