

**DARPA Tech, DARPA's 25<sup>th</sup> Systems and Technology Symposium  
August 9, 2007  
Anaheim, California  
Teleprompter Script for Dr. David Honey, Director, Strategic  
Technology Office – Networks Presentations**

Sharpening Networks into Usable Weapons

» **DAVID HONEY:**

Network Centric Warfare

– This is the key to enabling the COCOMs to achieve certain victory in an uncertain future.

You heard in STO's earlier session that we are seeking to deliver the tools the COCOMs will need to dominate the new strategic environment.

You also heard about the extreme unpredictability of the contingencies that the US military will face.

So, *how do we* respond to a threat that seems to evolve faster than we can build new solutions?

How do we get inside the OODA Loop of an adversary who is fleeting, adaptable, and willing to make any sacrifice?

We will do this with Network Centric Warfare.

This will be the mechanism that can blend capabilities already in the COCOMs toolbox, into a new weapon system capable of defeating our adversaries.

Network-centric warfare will enable our forces to quickly reorganize and implement new and decisive concepts of operations on-the-fly.

There are two key points about network-centric warfare that you need to know.

First, the key capabilities we need to implement network centric warfare *are here today and available to the warfighter.*

DARPA has taken the technology excuses off the table.

As you will hear from the other speakers in this session there are still opportunities to advance the state of the art, and providing leap-ahead capabilities *will* require further advances.

However, the fundamental capabilities needed to employ network centric warfare now exist.

Second, DARPA has clearly proven in field demonstrations the transformational capabilities of network-centric warfare.

We have shown in soldier run exercises that the network can enable commanders to combine weapons systems in novel ways and defeat unanticipated threats.

We have also seen that DARPA's network tools enable military organizations to transform and reorganize into more effective combat units.

The networking systems that DARPA has delivered to the battlefield in the last two years do far more than just move data.

These tools have changed the way that warfighters operate.

Thanks to *these* innovations, the network is becoming the most important weapon system on the battlefield.

Let me give you some examples that illustrate these points.

One of the most important transformational powers of network-centric warfare is the ability to link existing weapons and create entirely *new* military capabilities.

As part of the Silent Hammer exercise on San Clemente Island the Navy deployed Wolfpack, which is the DARPA-developed unattended signals collection and jamming system that operates as a self-assembling and self-managing network.

On its own, Wolfpack was able to detect and map RF signals in the target area, and relay this to a submarine-based command post.

The sub was then able to vector an EA-6B jamming aircraft to suppress the signals in the target area that Wolfpack had detected.

In the Cold War days such a capability would have been unaffordable for use by tactical forces.

However, by cutting Wolfpack's unit price from \$50,000 to \$500 per unit over the past year, every military service can now afford this transformational networked weapon system.

Another very impressive push of network centric warfare capabilities out to the tactical edge comes from the TTNT and QNT projects, both of

which are managed by DARPA's Information Exploitation Office.

These subscriber-based systems provide pilots, UAVs, and troops on the ground complete, current, automatically updated information that is tailored to the operations and missions of each user on the network.

The result is a unique and unprecedented degree of collaboration among dispersed units and dissimilar weapons systems.

With TTNT and QNT, fighter aircraft can use data gleaned from on-board sensors to generate targeting indicators for other aircraft, UAVs or ground units.

Similarly, ground units can immediately distribute time-critical intelligence or request and coordinate close air support.

A second important transformational aspect of networks is illustrated through the ability of combat forces to reorganize in the field.

We're already seeing this kind of network-facilitated organizational transformation in one of DARPA's greatest success stories – CPOF, or the Command Post of the Future.

With over 1000 CPOF units already deployed in Iraq, CPOF successfully transitioned this past year into a Program of Record for the U.S. Army.

CPOF permits commanders in widely dispersed locations to participate and collaborate in the planning and execution of military operations.

But, beyond this, CPOF is also flattening the military command structure and speeding execution.

For example,  
using CPOF, a battalion from one division can directly request support from a battalion of another division without involving the hierarchies of both divisions – turning what was formerly a 5-step process into a single step, while still ensuring that all intervening command levels remain “in the loop” and able to intervene if necessary.

From the theater level to a larger, national plane,  
we see this kind of network-enabled organizational adaptation collapsing one of the most traditional military organizational distinctions – between the J-2 and the J-3.

Breaking down the distinction between surveillance and intelligence on one hand, and operations and post-strike assessment on the other, is a profound example of the transformational power of networks.

The last few years of U.S.  
combat experience have revealed another new and unanticipated aspect of network-centric warfare.  
From now on,  
the outcome of combat will increasingly pivot on the ability of *our* networks to defeat *our adversaries'* networks.

We've learned that our adversaries aim is to counter *our* advantage in kinetic lethality with *their* version of ad hoc,  
self-forming networks – consisting of improvised combinations of commercial communications,  
the Internet, and  
human contacts.

For *our* network to beat *their* network,

*our* networks need to function as more than just tactical enablers for our traditional advantage in kinetic weapons.

We need to give the dismounted warfighter easy access to comprehensive, accurate, actionable information for rapid decision making and effective action.

The types of *information* required for success are becoming more complicated and more non-traditional in nature.

Commanders will always need to have an accurate picture of enemy positions, as well as friendly units and allies.

But increasingly it's social, cultural, political and economic information, foreign language capabilities and other clues – that are proving essential to the dismounted soldier.

To deliver this kind of support to the soldier requires us to overcome the next great challenge of military networking: developing *information-driven networks*.

*By information driven networks* I mean achieving for the warfighter, in an information driven environment, the kinds of superiority that networks now deliver in the kinetic warfare environment.

We must take information and knowledge off the table as impediments to timely action, just as we have already taken the technology excuse off the table for network support to kinetic warfare

Up to now, our networks have mainly addressed the central problem of kinetic warfare:  
putting steel on a target.

These networks have been used heavily in an interchange between intelligence personnel and military operations planners to achieve target destruction – kinetically.

Now users will require networks to help them solve -- minute by minute, in the field -- a variety of complex problems in chaotic military and civilian environments.

Delivering such extensive support to the warfighter requires us to fundamentally redefine the concept of the network.

Both the user and the provider communities – all of us, in fact – need to begin thinking of military networks more like we think of the internet – not in terms of the equipment and connectivity that make it work, but in terms of the tremendous range of services we can access through it.

These new services will mirror the traditional functions that are found in kinetic weapons based network centric warfare, which includes: Shared Awareness; Collaboration; Synchronization; and Effective Decision Making.

The difference is that the new strategic environment will require that warfighters at all levels quickly solve problems in a hostile environment that is laden with unanticipated political, social, cultural, and military complexities, and that may require a non-kinetic solution in order to achieve lasting success.

We need your help in uncovering new applications and services so that networks can provide US warfighters the resources they need to master the new strategic environment.

As we work toward information driven networks, we want networks

intelligent enough to provide, automatically, tailored information support to users at all levels – from Generals to privates – that responds to the particular location and mission that each user confronts.

We want networks agile enough to access and transmit useful information in a digestible form to users regardless of where that information resides on the network – at the edge, at the core, back in Washington, or in some other agency.

We want networks with the capacity and dexterity to provide users with both traditional military information and the non-traditional social, cultural, political, and economic information that's increasingly proving to be mission-critical.

And all of this must be done *fast!*

We must make sure that information availability isn't the "long pole in the tent", impeding timely decisions and actions.

While we are still a long way from such an information-driven network, some of STO's other networking success stories are providing the foundation for the information-driven networks of the future.

For example, we demonstrated our Network-centric radio system in 2006 at Fort Benning; this showed our ability to dynamically reconfigure communications during field operations.

This system allowed units equipped with different generations and types of analog and digital radios to seamlessly communicate and

interoperate.

Subsequent tests at Fort Bragg in December showed that this system moves data at far higher rates than any existing alternative.

Another STO success story – XG – has demonstrated an unprecedented capability for tactical communications by opportunistically exploiting unoccupied parts of the spectrum to connect users on different frequencies into one, self-assembled network.

Last summer in a demonstration test at Fort A.P. Hill, XG allowed users to instantly find each other in a fully assigned RF environment – even in the face of malicious interference, and without interfering with local, non-XG systems.

STO's Disruption Tolerant Networking has shown that our tactical networks can overcome the data transmission disruptions that are caused by foliage, terrain, jamming and congestion.

And STO's Wireless Network After Next program will provide the dismounted soldier with an affordable 4-channel, networked radio, incorporating all of the spectrum efficiency of XG with the robustness of DTN.

These network-centric tools will provide U.S. soldiers the ability to perform a wide variety of tactical missions and to operate effectively in hostile environments.

Unfortunately, these powerful, transformational networks are also prime targets for enemy attack.

To solve this problem STO also undertakes major efforts in Information Assurance and network defense for DOD.

Our Dynamic Quarantine of Worms program exemplifies these efforts.

In this particular program we aim to enable U.S. networked systems to rapidly self-recover when hit by a zero-day worm attack, and then inoculate our other systems against re-infection.

These programs and STO's other networking and communications programs all underscore that DARPA has taken the technology excuse off the table when it comes to network-centric warfare that supports traditional kinetic weapons systems.

However, we need to get busy developing information-driven networks to give our forces the ability to operate in a fast-paced, dynamic environment, and to defeat our adversary's informal, ad-hoc networks, without drowning in a glut of unintelligible information.

That is our next big challenge.

And this is where you come in.

We need your revolutionary ideas and inspirations to create true *information-driven networks*.

And, we need your ideas on how to make them robust: to defend them and to make them as secure as we possibly can.

Now that you have heard the STO Network vision,

my teammates will describe to you in more detail the main thrusts of our networking efforts.

If you have stopped by the STO booth then you have seen our technologies first hand.

STO's PM's have delivered unprecedented capabilities to the US warfighters, and I hope they have inspired you to step forward with the ideas that will enable us to conquer the next great frontier of military networking.

Thank you!

To start the Network presentations, I'd like to introduce Tim Gibson.