

I'm Dr Paul Kolodzy from the Advanced Technology Office.

I am here today to describe to you an exciting new program: WolfPack!

I'd like to take the next few minutes to describe how the WolfPack Program will add a new dimension to Electronic Warfare.

The WolfPack program was an ATO new start program this year.

Its goal is to develop the technology to disrupt communication links by using networks of jammers.

Like a pack of wolves, the power comes from the group behavior of many small units over a single, powerful unit.

As I indicated, WolfPack is being developed to deny the enemy the use of radio communications throughout the battlespace.

That is, from 20 MHz through 2.5 GHz.

We will attempt to accomplish this through the use of a network of low-power jammers.

In order to bring the weight of the entire group to bear on the enemy, these jammers must operate automatically and in cooperation with each other.

All of this must be accomplished without disrupting friendly and neutral radio communications.

As you have heard, and will continue to hear throughout this conference, we depend heavily upon our ability to communicate!

Any offensive system cannot be allowed to adversely affect our own systems.

Current standoff systems use high-power and directivity to accomplish their task.

WolfPack trades those attributes for short-range and selectivity to target signals.

This provides new opportunities to locate and characterize emitter nodes and their communication nets.

As the energy emitted by future radios continues to drop, standoff systems will have a much harder time hearing the signals.

As the number of radios continues to rise, standoff systems will have a much harder time distinguishing one radio from another.

WolfPack will solve those problems by being CLOSE, DISTRIBUTED and NETWORKED!

The WolfPack concept envisions a mission of tailored mix components incorporating the various system functions.

The first function will be ESM collection to listen for radio emissions and then identify the type of radio.

ESM collection is optimized by emplacement in advantaged positions.

Trees, hills and structures block many of the radio transmissions and an elevated position will make it easier to detect signals.

The second function will be to transmit the jamming and confusion signals.

These signals will deny the adversary clear radio communications.

These units require a higher density distribution and closer proximity to adversary units.

The final function will be to monitor the status of the units and coordinate the actions between the individual units.

This function could be contained in a few highly advantaged units with superior location and processing power.

They will map the battlespace emitter picture and determine the reaction of the overall WolfPack system to an enemy activity.

Lets talk a little bit about the distributed jamming concept.

We are going to employ a close-approach jamming concept.

This allows us to look at using low-powered units to effectively deny enemy communications.

Being close helps us detect and classify radio signals. At closer distances, it is easier to determine radios by signal strength.

Thus the ESM units can conduct very effective signal collection and location reporting.

One of the basic questions is: "How close do we need to be to the adversary?"

That depends on the mission.

The mission will tell us if we need to place the units very accurately, within 100 meters, or coarsely, within 1000 meters.

There are many systems that can be used for putting the units in the field at these accuracies; such as Free Fall devices, smart munitions or Unmanned Air Vehicles.

Another way to look at close versus far is in the physics.

Comparing the WolfPack system to a standoff, airborne system should provide some insight.

The goal is to jam a 50W radio link, say on a vehicle.

If we use a standoff jammer at 50 km, then we would need to transmit 50kW of power!

That's a lot of power!

And even with that much power, you would be effective less than 70% of the time.

Now replace power with shorter range.

Now, if you place the jammer within 1 km of the vehicle, then a 10W or smaller jammer can do the job.

That's a lot less power!

And to make matters worse, as you increase the power on the standoff jammer, you increase the risk that you will also jam a friendly or neutral radio network.

These fundamental advantages motivated us to seriously look into distributed jamming.

Now lets talk about the target signals of WolfPack system.

First of all the WolfPack system has to be agile.

What I mean by agile is that it has to sense and react to a wide range of signals.

And it has to do that in near real time and in all sorts of environments.

It must be capable of attacking a wide range of communication signals.

It must handle strategic, wide area system signals.

It must handle tactical, wide area signals.

It must handle all the individual systems such as air defense nets, close air support nets, and Combat Net Radios.

We have looked at the full range of signal types.

Our current thinking is that Combat Net Radios prove to be the most challenging.

Why?

Because, they use anti-jam waveforms and move around quite a bit.

So we made the Combat Net Radios the initial focus of this program.

However, a recent assessment of other mission areas has provided some interesting results.

One potential mission is defeating advanced IADS RADARs.

This new mission appears to offer additional opportunities for the concept.

Now let me go over the three basic application areas of the WolfPack system.

The first is the electronic counter measure mission.

We have depicted the ECM mission scenario with red vehicles and their associated radios.

The WolfPack units are the small blue diamonds across the battlefield.

The ultimate objective for WolfPack is to deny an adversary the use of their communications system during critical phases of battle.

If they cannot communicate, then they cannot give commands or provide reports.

That would seriously impact the Command and Control capabilities of the enemy.

Without timely command and control, it is very difficult to coordinate your forces.

Advantage WolfPack!

This is accomplished by placing units in advantaged positions to collect transmissions and to analyze and characterize the enemy's networks.

One of the Wolfpack nodes, as depicted here in the tree, will detect and characterize the communication activity.

The detection node, using the communication network, will provide this information to the distributed jamming nodes.

WolfPack will then react in one of three ways.

In this example, one or multiple jamming nodes will attack the network to prevent link closure.

Wolfpack can also confuse the enemy by providing misinformation into their radio transmissions.

Or, have the detection node simply report the emitter activity and location to other systems.

The second application is NOT to deny the enemy the ability to communicate, but to prevent the enemy from exploiting OUR communications.

This is the Electronic Counter- Counter Measure mission.

In ECCM, we will create a sort of "cocktail party" effect.

Similar to you trying to hear someone across the room during a party, we will increase the noise level around the enemy receiver making it difficult to hear our radio communications over all the background noise.

In this application, the listening units are again placed in advantaged positions.

This time they are analyzing both the radio transmissions of the enemy and friendlies.

That is shown here by the emanations from the red vehicles listening fro the BLUE communications.

Here the network plays an important role.

Some of the nodes will detect the RED activity and some will detect the BLUE activity.

The communication network will allow the SYSTEM to understand the entire communications picture.

When directed by the Blue Commander, the WolfPack units will raise the noise floor around the Adversary receivers.

This will prevent the detection of friendly force communications by enemy collection systems.

In this way, you are putting more noise local to the unfriendly receivers.

And therefore they will not impact Blue transmitters, which are at a greater distance.

The last application is to disrupt enemy Air Defense Systems.

We call this the Distributed Suppression of Enemy Air Defense, or, DSEAD mission. This requires us to design WolfPack to work at higher frequencies such as 2.5GHz to 15 GHz and beyond.

In this application, WolfPack would respond similar to the Electronic Counter-Counter Measure mission. WolfPack would provide cover for friendly aircraft by jamming air defense nodes.

The difference in this mission is that WolfPack can target either the radar or the communications links.

Our assessment suggests that the proximity of WolfPack provides an extraordinary advantage in overcoming enemy RADAR counter measures.

WolfPack will overwhelm classic methods such as Sidelobe cancellation.

We will do this by having the WolfPack units detect and determine the exact location of the enemy RADAR system. As the system is identified, WolfPack will respond in one of three ways:

- 1) they can prevent radar communication with the fire control system.

If the radar cannot tell the missile to launch, the system is compromised. Advantage WolfPack!

Or 2), as shown in this depiction, they can jam or confuse the RADAR. If the radar cannot see the aircraft through the noise, then it cannot tell the missile where to aim. Advantage WolfPack!

Or 3) as with the previous missions, WolfPack can provide precision targeting information of the enemy radar to the Blue commander. Advantage WolfPack!

Now let us review the technologies to enable these three missions.

In the next year, we plan on investing in enabling technologies to bring this concept to reality.

In that vein, this program provides an extraordinary opportunity for the enhancement of state-of-the-art technologies.

These include RF signal detection, digital signal processing, and network characterization. This will be a very unique program trying to take on all of those challenges.

Now, I will walk through the WolfPack operational timeline, and its associated technical challenges.

The RF Intercept stage is where it all begins. This stage will require new designs in Analog-to-Digital (A/D) converters, low power front-end processors, and antenna designs.

We are going to need systems that are low power, highly dynamic and hard to find.

The next stage is the signal processing stage. This is where classification techniques are used to process intercepted signals.

There are many initiatives that are researching various classification techniques. WolfPack will use those techniques as they evolve to address new threats and systems.

As the technology matures, they will be integrated with the WolfPack processing stream.

The next stage is locating those signals once they have been detected and characterized.

This is where the network will play an important role.

WolfPack will provide a precise location of the emitting signals in real time.

We believe this capability will become critical in the future when our adversaries will have a greater dependency on radio communications.

As wireless networks proliferate, it becomes more important to characterize and attack the critical points in the network.

This is where the distributed network nature of the WolfPack concept comes into play!

The WolfPack network will be used to provide data on enemy transmitters.

A challenge is how to stitch together this information to form a picture of the entire enemy network: its form, its function, and its vulnerabilities.

This will fundamentally change the way we attack communication systems.

We can then contemplate surgical strikes of critical elements of a network.

Next, we determine WolfPack's response.

As I described before, the response can come as jamming the communication system or just reporting the location of that system.

The technology developed for this stage will determine how sophisticated WolfPack will be.

Will WolfPack respond to some operator far away or will it be an independent operator?

That depends upon how reliable we can make the response algorithms.

Remember, we want to do no harm to our own systems!

And finally, WolfPack is ready for action!

We are finishing the first year of the WolfPack program.

In this first phase we worked as an Industry, Academia, and Government professionals Tiger Team.

The Tiger Team drafted the conceptual architecture, studied critical tradeoffs, and made comparisons with stand off systems.

This initial work is nearing completion.

Next year we begin investing in the enabling technologies.

The following years will be devoted to developing components and initial prototype systems.

Our goal is to field-test the prototype WolfPack units and operational concepts in 2004.

To begin the next step, we are holding a WolfPack Industry Day in Washington within the next few months.

This meeting is for potential bidders of the enabling technology portion of this program and we will be providing the phase one-program results.

This is an excellent opportunity to meet with members of the Tiger Team and me.

This concludes the formal portion of my presentation and I look forward to visiting with you on this and other subjects during DARPA Tech and in the future.

Let's have fun developing technology!