SECURE, DYNAMIC, ROBUST, AND RELIABLE NETWORKING

Speaker: Colonel Tim Gibson

In the Network Centric Warfare environment we envision for tomorrow's battlefield, having the best possible technologies is paramount. If we cannot talk and pass data on the battlefield, the idea of Network Centric Warfare just will not work.

This is the case because fortunately ... or unfortunately, depending on your point of view ... networked systems are everywhere in our military. The U.S. military has embraced networking with amazing speed. Our strategic doctrine for the last few years has been built around new tactics based on the idea that "the Network is the Weapon." Our commanders and soldiers are planning on the network being there. A very important question is "Will it be there for them?" Assuming it is there, what is that network going to look like? What do we need? Those questions, and their answers, are what I'll talk about for the next few minutes.

Our current methods for securing systems are not working well. We must find a better way to secure our computing systems and digital networks. An aspect we need to push hard in is "practical security." We need to solve our policy and technology problems for sharing and protecting information in practical ways ... not necessarily perfect ways. A fair amount of the technology we developed in the last decade is neither practical, nor reliable, nor scalable. A good example is the Public Key Infrastructure, which is difficult to implement and does not scale well, but has perfect mathematical functions. Any number of proofs exist to show that it works perfectly ... on paper. We also have a nice fixation with the Holy Grail of computer security, having a true multilevel secure system. Golly, wouldn't that be a nice thing to have? Well sure it would ... but we've been at it for twenty years and haven't got it right yet. So ... can we get on solving with some tractable problems? Our military needs good security now, not perfect security ten years from now. Commanders are tired of the waiting and the promises. We need to give them good security solutions now, because otherwise they WILL use whatever they have to get the job done.

We need communications and networking equipment that has four basic attributes: Secure, Dynamic, Robust, and Reliable. It may seem a little strange that I list security first. That may be because I was an Infantry officer first, a computer officer second, and have seen first hand how things work in the field in both jobs. The priority for soldier is to get the job done. You do that with the best and safest ... or most secure ... tools available. If the best tools are not available, you do the job with what you have at hand. If the tool is not secure, you secure it as best you can, and move out smartly. If it is insecure but you need to use it, use it carefully. Unfortunately, soldiers, sailors, and Marines don't always know how careful they need to be. They think they know, but they may not. This is the same predicament the Germans, Japanese, and Italians found themselves in the Second World War, and we do not want to ever be where they were at that war's end.

The Germans and the allies used variants of some very nice encryption machines called Enigma and Geheimschreiber; these machines supposedly generated an unbreakable encryption scheme. Fortunately (for us anyway) the Allies did not find them unbreakable. Breaking the codes gave the Allies insight into the enemy's strategic and tactical moves, wartime production, and many other things ... the code breakers were essential to winning the Battle of the Atlantic against the U-boats. Why am I telling you this? Because the code breaking early in the war exploited human errors

combined with a slight weakness in the machine. Either would have been an annoyance, nothing more. Together, they were crucial to breaking the code. When the Germans and Japanese changed their operator procedures to correct the errors and modified the machines to make them more secure ... it was too late ... we knew how the machines worked and were able to break the codes regularly for the rest of the war. Re-enacting this scenario today, with our computer networks playing the part of the Enigma machines, is something to lose sleep over.

I mentioned reliability and dynamic, so let's look at each of those in turn. First, "How do we know if we are making a difference?" with reliability?

Take a good look at how the military uses computers. We use these systems the same way we used them ten years ago. You do find them in a lot more places than ten years ago, but they are basically doing the same things. Maybe it is a little different, but not much. We certainly do not use our computing resources to their full capabilities.

What am I talking about? Well, look at a couple of Internet behemoths, Amazon and Ebay. Both of them make money, and neither could function without the Internet. If the Internet stopped tomorrow, they would cease to exist. Now I am not saying the military must be totally dependent on a network ... that would be a bad thing. But I am saying the military should reexamine its span of control, organization, and basic operational concepts if they are going to fully exploit computers and networks.

If you want an example, consider our current ground force organization, the triangular division. This division structure replaced the square division in the 1920s. We have used the triangular concept successfully in the Second World War, Korea, Vietnam, Afghanistan, and two wars with Iraq. You get with a winner and stick with it ... right?

In the last eighty years communications, record keeping, and sensor technologies have gone from field telephones to powerful radios and satellites; paper records have become powerful handheld computers; and the biplanes of the 1920s are now UAVs. This is an amazing amount of change, which makes our organizational rigidity even more interesting. All this technological change ... and investment ... and yet we still use the same organizational structure. Why?

Is it because the commanders and users don't know what they have? Are they just stubborn? Maybe they're stupid? Maybe ... No, the answer is that in order to rely on a technology so strongly that you are willing to change how you fundamentally do your job ... also means you must also be able to RELIABLY predict how that technology behaves. The flintlock musket replaced the longbow as the primary infantry distance weapon in the 1600s ... even though the musket's accuracy and rate of fire were many time worse ... musketeers took less time to train than bowmen. Training time was cut by over 90%, from six years to one month. The slower rate of fire and poor accuracy of the musket were acceptable tradeoffs because Commanders knew exactly what they were getting and were willing to make tactical changes based on capabilities. QED.

Modern networks provide commanders with incredible improvements in communications, as well as vastly improved data collection and analysis. We can get the commander better information

more quickly than ever before. So why do they use the same organization? Perhaps because they are stuck in the status quo and are just unwilling to change. Perhaps ...

On the other hand, it may be that while commanders are willing to use these new capabilities, they are also unwilling to rely upon the new systems because these computing systems are inherently unreliable.

Think back to your office or home computer. How often has it stopped working for some mysterious reason? How often has it appeared to work but "was just kidding." For example it seems to send mail but you find out four hours later the mail was never delivered? Now compare that to your home telephone. You go to Wal-Mart, buy a telephone for less than $10, plug it in the wall, and expect it to work. Expect ...

Expect to work ... that is a phrase I have never heard anyone use when talking about computing systems. We do not expect them to work; we expect them to have a problem. If commanders expect a system to have a problem, how can they rely on it? How can you change your organization or alter how you fundamentally operate on the basis of something that 'usually works,' at least most of the time?

If we want to have a true impact on the military, we need the computers and networks to be more reliable. We should be much closer to five '9s' than our current nine '5s.' Part of this reliability must be how the device communicates with the user. A blinking cursor is not constructive. A different busy signal to let you distinguish between a busy number and busy circuit on Mother's Day is helpful. We remembered to build functionality into the telephone system; what happened to the computer networks? If a person is unable to use a system the way they want because of a problem, the system needs to tell the person what the problem is ... in clearly understandable ways.

Practical, reliable, and dependable. That's how our systems need to work. And going back to my first point, that's how our security needs to work too.

Dynamic. On tomorrow's battlefield, being dynamic isn't good enough. Any network must also be scalable to larger or smaller sizes. So, what we really need is ... dynamic scalability.

Today's networks look like this. Stationary networks with a static infrastructure that provide service to fairly static end nodes. Mobile nodes tie into the static infrastructure. Moving a node outside of its normal service area usually means reconfiguring something. Moving the infrastructure always means reconfiguring something. Our security devices are configured to protect these static networks.

The static network is no good because on tomorrow's battlefield, everything will move around all the time ... frankly we are not ready for that. While we have made some great strides with mobile ad hoc networks, cellular telephones, and wireless computer network protocols, nearly all of these concepts are tied to stationary service points.

Tomorrow's military networks will constantly move from one place to another, always reconfiguring their connections and topologies. They may shift from tactical radio to fiber-optic

connections to satellite ... or they just steal, sorry, I meant "borrow" bandwidth from a tactical wireless network that just happens to be driving by on a convoy. They need the flexibility and trust amongst themselves to do that. They must be dynamic.

The partner of dynamic was scalable. What does that mean? It means that we can experiment with small ad hoc networks that can dynamically configure themselves, but those techniques may not work with the communications infrastructure of division's worth of soldiers or Marines ... each with their own personal network. That is an entirely different kind of problem. That is the problem we must solve.

So, let's put all of these ideas together ... secure, dynamic, and reliable. While DARPA has been engaged in a number of programs that have in the past ... and will continue in the future ... to vastly improve our ability to use tactical communications, there are a number of inherent problems that are forcing us to adjust our thinking. Changing topologies ... short deployment periods ... the availability of sophisticated countermeasures ... the normal challenges of military operations ... all of these factors ... and many more ... will impose limitations on our communications, and we must solve these limitations.

The last thing I mentioned at the beginning of this talk was robustness. In the simplest terms that means having a rich set of features our current networks cannot have. We need things like levels of precedence ... where important transmissions can bump lower ones ... and levels of service built in. On the other hand, I did not say Quality of Service. Why not? Because the packet network paradigm probably needs to change.

The Internet Protocol, and it does not matter what version you use, works on a probabilistic delivery system. If you send something it probably gets delivered. If the message doesn't make it, you probably find out about it. Probably ... squared. Great. Now is that something you want to bet lives on?

I am not advocating completely throwing out the Internet Protocol completely, but we must absolutely have a mechanism for assigning network capabilities to different users that scales to large numbers of devices automatically. A commander wants to be able to send a message and have it delivered ... completely, accurately, and on time. If it does not get delivered she needs to know about it. If someone else needs to have their transmission slowed, or maybe even be preempted, to make that deliver happen, so be it.

We have looked at solving this problem before. But the methods we have developed to date do not scale for large numbers of users. One recent solution only requires us to reload all the software on the Internet at one time and reboot the entire thing. We did that once ... a long time ago ... when there were less than 100 ARPANET hosts ... but it is not practical today. To repeat what I said earlier, we need something in this area that actually works and scales to large numbers of dynamic devices ... securely... and reliably.

When it comes to realizing the military's goal of Network Centric Warfare, we are in a race. Our military commanders deploy new technology as fast as they can get it. Many military programs

assume that new network technology will be there to support them. Unfortunately, it may not be there. This is the challenge DARPA must rise to ... and why we need your help.

We must challenge the technical assumptions that underlie today's Internet and face up to its limitations. Many engineers and scientists are doing outstanding work to improve our existing IP technology, and the military will benefit from their work. But that work is not good enough.

We are looking for revolutionary progress ... evolutionary will not do for tomorrow's military ... and providing "the next step" has never been DARPA's role.

The four things I talked to you about to day, security, dynamic, robustness, and reliability will provide the military with the communications networks we need to win tomorrow's wars. So, what are the DARPA hard challenges?

Security. Period. No compromises, no prisoners, no questions. Because if we cannot trust an information system it should not be used. Worse, if we use an insecure system because we have to; we may be winning a battle, only to find ourselves losing the war.

Next, our networks must be reliable. They should work, all the time. Commanders should know the network will be there, expecting it to work. And if it is not working, we should know the reason and the consequences.

Dynamic. It should not matter how big the network is or who is in it, it should still work. It also cannot matter if everything is moving around. The network must scale even if all the pieces change places.

These are the networking problems we need to fix at DARPA. They are the same ones we need your help on. We stand ready to work with you to make tomorrow's military a better fighting force. Because on tomorrow's battlefield ... if we rely on a computer ... it has to work right, the first time.

Thank you