Lee Hutchinson: Welcome to the first of two special editions of the Ars Technicast. I'm your host, Senior Technology Editor Lee Hutchinson. Our discussion today is going to focus on the internet of things, but not the usual internet of things. Today, we're going to talk about the internet of military things. For at least a couple of decades now, the US Department of Defense has been trying to make the tools we use to fight battles more like the tools we use in peacetime, with more connectivity, more data, and more smarts.

The difference this time around though, is that technology has caught up to the point where what we can do in real life almost mirrors what we can do in movies. Sticking sensors and data on everything in the battlefield brings a lot of challenges, and we're going to talk about those too.

My guest today is retired Air Force Brigadier General Scott Stapp, who is currently the chief technology officer of Northrop Grumman. Scott knows a ton of stuff about the shape of the modern battlefield and he's going to share that knowledge with us.

Scott, if you could give us a little bit more about what you do, because your bio is extensive.

Scott Stapp: Sure. Thank you, Lee. As you said, I am the corporate technology officer for Northrop Grumman. I've, believe it or not, only been in that position a couple months. I've been with Northrop Grumman for about six years. I started off running research and development for one of our sectors in the company, looking at both air and space. I migrated to a business unit where I worked in this new resiliency rapid prototyping world to look at how we're going to leverage space for our future customers, and then have since moved to the CTO role for Northrop Grumman. Prior to that, I did a 30 year career in the United States Air Force where I did really acquisition engineering and flight tests.

Lee Hutchinson: Excellent. Thank you for your service, sir. We have a very broad topic in front of us today, but it's one that I think you're uniquely positioned to discuss. The typical Ars Technica reader is going to be very familiar with the concept of the internet of things, or IOT. Right? That's the gradual increase in the number of internet-enabled devices around the world, which is giving rise to a connected web of appliances and tools that are able to communicate with each other.

Now, the average Ars Technica reader may not be familiar, though, with how that same concept, the concept of the internet of things is being applied to the defense and military side of the house to create what has, for the last couple of decades, been referred to as the connected battlespace. That's sort of a buzzwordy kind of thing, but Scott, can you set the table here for us with defining what exactly that is when you say connected battlespace and bringing us up to where we are right now with that? What is it, what does it mean, and where are we?

Scott Stapp: Connected battlespace is exactly as you would think about the internet of things. I think one of the issues that people will struggle with is the internet of things has been around so long that it is just second nature for everyone to understand that their phone is connected to their bank, which is connected to their doctor, and they can send x-rays, and everything is just connected.

The DOD has not operated like that or actually been set up like that, and in a lot of ways we still operate decades behind what we had done. In fact, what I would say is we operate almost like, I would say, subnets or local area networks versus a wide area network. You may have a set of fighter aircraft that talk to each other and they can communicate, but they can't communicate to anybody outside that. You might have a set of ships that can talk within their bubble, but they can't talk to anybody outside that bubble.

When we talk about an integrated battlespace, what we're starting to see is that we need an ability to actually connect all of our services together: army, navy, air force, marines. We need the intelligence community tied into that, and we need that data to flow freely from everybody. In a lot of ways, what I would say is it's crowdsourcing your own elements within the Department of Defense and intelligence community to make that data available to everybody.

Lee Hutchinson: That sounds like, not to put too fine a point on it, but a very difficult technical challenge, because you've got... Things move slowly in the Department of Defense. You've got decades of legacy systems talking, different protocols and everything. I have to assume that unifying all that is like a pre-step that you have to take before you can even think about any kind of integrated comms.

Scott Stapp: You just hit number one with the issuance. Right? For anything to communicate together, you have to be at the same frequency spectrum. You'll find out that we have different data links, air to air, data links that go air to ground, air data links that go ship to shore or vice versa. In a lot of cases, those data links do not operate in the same frequency spectrum.

The other issue you have is, even if they did operate in the same frequency spectrum, what you have is you have different protocols. They have different messaging formats, they have different encryption standards and algorithms. At some point, the real option is you either get on the same standard, which is going to take a very long time. We will work with all of our customers within the US Government to actually start coming up with that common standard. But in the interim, what you're really doing is you're looking to try to do point to point with almost translators that will actually translate a message format A to message format B with no latency lag so that people can get that same information in their current format.

Lee Hutchinson: I know this concept here is something that has been around conceptually for a long time, and in fact we've, the United States, has tried to do stuff like this before. Right? The current effort to build up this new connected, integrated battlespace, like you said, this is not the first time we've tried to do this, right?

Scott Stapp: No, it's not. You had future combat systems back with the army. I will tell you, that wasn't a joint effort. That was really trying to interconnect the army's battlespace. The joint staff in what they call the JROC, the Joint Requirements Oversight Council, tried to set a baseline requirement. What they would call a key performance parameter that was called Netcentric. This was established probably 10, 15 years ago. In fact, at that point, I had run the JROC for a period of time and people didn't quite understand what Netcentric meant. What they're really starting to see is what it means is this internet of things. It's really this internet of war fighting things. When we do what we want to do is called joint all domain command and control, an ability to control your battlespace across multiple services. You can only do that if you're actually talking to each other and connected.

Lee Hutchinson: This can extend all the way to instrumenting very tiny things on the battlefield. We're talking about the addition of sensors into areas that don't necessarily have any sort of data gathering ability in them right now in order to make the things that all these individual systems are doing visible up the command and control chain. Is that accurate?

Scott Stapp: Completely. What's funny is even when the internet of things started, it really started as an ability to communicate and push what I'd say is a standard of email or documents back and forth. What it's transpired into is your ability of your phone to watch TV, make phone calls, pay your bills, actually send x-rays for medical. It can watch your home, connect to your ring device. No matter what device or how small, it allows you to connect to everything that you want to command and control. The construct of command and control is not a unique thing. Every human being does that. In my life, I can command and control my bank account. I can command and control, hey, I can go buy movie tickets, I can talk to my doctor. I can go to another doctor and actually have my medical records sent over by me through that same device. I can command and control that sub-element of my life, and then we all have, like for me, I have a superior commander, my wife. If she is off the net, so she has cell coverage, but she...

PART 1 OF 4 ENDS [00:08:04]

Scott Stapp: And if she is off the net, so she has cell coverage, but she doesn't have internet, she can direct me to go buy movie tickets, at which point I can buy those. And when she gets back in the net, they auto-populate into her device. We're really talking about is the military is just looking at doing that exact same thing, that no matter what the device is, if it is a data collector, if it is sensing something ... so you can imagine we have a lot of space systems. It gives you global coverage if you can map that global network. So what I would use is I'd say the same thing as Ways.

So as Ways does crowdsourcing of those who are in it, and they can say, "Hey, there is a police officer here, there's an accident here," these different elements, as the space systems start to register different activities, they should be cross correlating with each other and essentially crowdsourcing all of our

sensors to give you some fidelity of what the battle space looks like. That then ties back to the war fighter, who is really looking at how to engage that battle space, where everything is, how to coordinate it. And actually, what we're looking at doing is you will tie in artificial intelligence and machine learning so it can optimize which weapon systems get tagged to which issues in the battle space.

Lee Hutchinson: So this brings up an interesting question, actually, and it's one that even reading over the materials here, I've really wanted to ask. And I know it's not a question you can fully answer, but maybe you can help sort of give the shape of that answer. For home users like me, when you look at internet of things devices, it's cool how you can have a thermostat that talks to your refrigerator or whatever, but the more connected devices a typical person has in their home, the broader their attack surface becomes, especially with consumer devices that may not be put together as well as they should be or programmed as well as they should be and that may not get updates, et cetera. This is a real problem, I would imagine, with the connected battle space. As you broaden the number of signals you're sending and receiving everywhere, you broaden the potential attack surface for your adversary. So how is that dealt with?

Scott Stapp: Okay, so you've hit the number one problem that both the industry and the government are going to deal with over time. And in fact, actually, the reason our current systems and our data links are designed the way they are, is to prevent exactly that. If you make them restrictive enough, they're only allowed to go point to point between a couple of people or within a flight of six or seven or eight aircraft, you don't run the risk of somebody entering that net and causing disturbance. So the corollary is as we do this internet thing, we understand people can hack your life and get in and you get identity theft, but imagine if somebody could ... when they did identity theft, it could actually cause a fatality within your family. When somebody hacked in, it literally was a life or death.

And in the military, that's what they look at, because when somebody gets in your net in a conflict, it is now a life and death situation. So we're going to go, I believe much more cautiously and carefully, because that security element can't really be overemphasized. It's extremely important going forward. Now what I will tell you is we've recognized that you also run a risk by not doing it. By not being interconnected and effective, if you get into a conflict and an adversary has done that, if they've protected themselves and you can't get into their net, but they're really very highly connected and rapid and we are not, you run a risk there. So you're going to constantly have to balance these risks between higher connectivity, higher efficiency, and security. That will constantly be this balancing act that senior leaders will have to deal with.

Lee Hutchinson: I know that attacking an enemy's command and control structure traditionally is always a good military goal, but is the broadening of all of this access into command and control because of all these connectivity things that are happening, does that make this an even larger target? Both for us, and also ...

when I say us, I mean the United States. If we're on the battlefield, not only do we have to worry about defending our own command and control stuff now that we're in internet of things world, doesn't this also present us with a bigger, valid target for adversaries who are going through perhaps their own large scale changes to integrate their own battle spaces?

Scott Stapp: It does, but not in the same way. So what I would tell you is this; I don't think there's any desire to have all the DOD command and control from one person at the very top. So it's not going to be a single command and control structure. What it really is, is I would say it's very ... again, back to the internet of things, is if you look at it, every company runs a sub-net on the internet of things. So even if you happen to hack into company A's network, it doesn't tie directly to company B's. There's different ways to get in, but company A and B can still share data, it just doesn't necessarily allow you a direct tie it. So what the DOD is going to be looking at is an ability to share data with a bunch of subnets, so what we would classically call centralized control, decentralized execution.

There will be sub nodes of command and control, but what you want that sub node to be able to do ... so I'll give you a perfect example, which would be a carrier strike group. A Naval carrier strike group has an aircraft carrier with a bunch of support elements that ships and air forces and ISR sensors, and they typically are looking at protecting that bubble of the ship. But what they want to do is be able to see beyond the horizon, beyond their bubble, and they need data to be able to feed in, but they will command and control that structure from within potentially that bubble. There's desires to look at how you might command and control from one bubble, essentially one battle bubble to another. And that's why when they talk about all the main command and control, there's two elements. One is the technical element, which is really you can't command and control anything you do not have connectivity to. If I do not have a connection to my bank, I can not make a bank transfer. So you have to have an ability to have data flowing.

The other element is more of a human element, which gets to if a space system sees a problematic threat way over the horizon that the Navy or the air force can't see, a space guy, if he has what we call target quality data, can he have the authority to launch a weapon off of an air force or Navy platform? That's the human element, of deciding who actually has the authority to do what. And that will be a long debate within the government of how do you effectively command and control assets that are dispersed all over? I think what industry really has to do is we have to provide them the connectivity to allow that debate to be more effective. Because again, if you're not connected, there's no use having the debate. You can't control it anyways. If we can start providing that connectivity of what we call every sensor to every shooter, is it allows them to have a more thorough debate on how you actually conduct the concepts of operations and the tactics, techniques, and procedures to do command and control.

Lee Hutchinson: It seems like there's also potentially something that you guys have to worry about overcoming, and it's that by giving all this information to the folks who are in the positions who need to make these decisions, by enabling the war fighters to be able to do those joint decisions, like you said, it feels like you have to walk a line here between giving people enough information and giving people way too much information, which in my recollection is that was one of the issues that the army found out when they were going through their land warrior program, was that at a certain point, the guys on the ground have enough to do without worrying about additional displays and screens and sensors and the commanders above them are potentially at saturation with the information they have available today. So how do you work that problem?

Scott Stapp: One of the biggest issues is information overload or data saturation. So human beings really struggle with massive information overload and we can tend to go into lock ... we just lock up. That's where I think artificial intelligence -

PART 2 OF 4 ENDS [00:16:04]

Scott Stapp: We just lock up. That's where I think artificial intelligence and machine learning really come in, so understanding, and just like any AI, ML tool, whether you play the game of Go, whether you play chess, you have to actually teach it, how you do operations, what's important? What's not? How an adversary may move or not, so that what it gives you is it gives you the information you need. Not all the information, because not all the information is important, and the one nice thing with commercial is commercial has burned down so much of this.

If you look at your standard Google search engine, when you start typing in, and it starts trying to predict what you've done in the past, and how you've looked at problems, a lot of that technology, and a lot of that learning has already been done, and what we have to do is port some of that over to understand how it applies in a DOD construct.

Lee Hutchinson: That's really interesting. Do you foresee that kind of extended cooperation between private entities, and the DOD when it comes to the machine learning stuff? Because, a lot of these companies, that's kind of their secret sauce, and they license it out, or they keep it internal at all. I would imagine that there are complicated issues here, if you're introducing some aspect of machine learning AI, I say AI, but we're not at AI yet, it's all machine learning.

But, there are complicated issues when you introduce machine learning into situations that traditionally you would always only have a person in the decision loop for, right?

Scott Stapp: No, absolutely, and again, that's why it really becomes a complex problem when you start talking about life and death situations. If you're playing chess or Go, and you can always repeat a game, it's not a huge issue, but what you also find out is it's hard to play a war game in reality, is everybody, every country,

adversaries, allies, everybody have what [Wukowski 00:17:54] called war reserve modes. They don't use them all the time. They only use them in conflict. The question is, how do AIML algorithms respond to unique upsets that occur that they have never seen before?

And, in a typical battle space the commanders want to have known outcomes, and that's why we test everything to death. What you're really getting to is not only that, but how do you test these elements? When I was a flight tester, as a air force guy, and you go out, and you fly test points, and you fly them over and over and over again, so you have a statistical analysis that says, "I have high confidence when I do this, it responds like that." And, it's just done all the time. The question is, with algorithms that learn in a changing environment, how are you assured to get the prescribed outcome, especially, when it's seeing variables for the first time that it may have never seen before?

And, those are things we're going to have to work our way through. I know the department of defense is struggling with that right now, defense industry is trying to work with them to figure our way through that, but right now there's no easy answer, and we're all kind of learning our way through it as we go.

Lee Hutchinson: Yeah, well, it's a hard problem. You know the advantage here that we can sort of back into the issue with the outcome, and we can train toward it, and yeah, I can see how this is like really difficult. Yes, we've been talking a lot about the theories, and the things that are behind this, but I want to ask from like a practical standpoint, folks like me who haven't ever served tend to have a very Hollywoodized, or I guess, call of duty eyes, vision of how a modern battlefield engagement unfolds. We've all played the games, we've all seen the movies. We have sort of a popular entertainment version of how much, or how little info a military commander has access to in the middle of a firefight.

But, from a practical standpoint, what does this really look like? Cast your eyes out here, 10 years, the joint all domain command and control, the JADC2, let's say it's operational. What does the different window that each layer of command has in the battlefield look like, that you've got from the squad level to the captain, to the colonel. What is each person seeing? They're not just like moving little guys around on their screen, like playing command and conquer or anything.

Scott Stapp: I don't believe they will, but I'll be honest, I think what we almost want to get to in some ways is what you're talking about, which is the Hollywoodized version, or the computerized version, because that's where I think most people have struggled with. I think, in a lot of ways, they think that's where we're already at, and that is nowhere near where we're at. Here's the question. Everybody who enters into the internet of things now, if I get on my computer, if I do anything, what I want to have information for is tailored to my needs, so when you say, whether it's at a squad level, a platoon, a company, a brigade, or in an air force, a squadron, what you want is you want it tailored to your needs, but what you want is access to everything.

Everything's connected, so when I plug my computer into the internet, I have access to everything, but I don't pull everything. I pull what I want and what I need. I think what you want is you want a squad, even on the ground to have access to as much as possible, and that squad commander, or a platoon commander actually tailors it to go, "Listen, I need information in this geographic region. I need it from this elevation to that elevation. I need it across this..." He can tailor what his demand signal is, and then, ideally it populates what he needs, so he can declutter if he doesn't want it.

So, he could look at an air picture, and decide, "You know what? I'm not really worried about the air picture, I'm going to declutter that and take that off my screen. I'm really concerned about the ground element, and I'm not even concerned about it behind me, I'm concerned about it in these coordinate areas, in this box, please show me everything that's out there." The idea is, he will be able to tailor what he needs for that construct. I think, one of the big elements, and this is where commercial has really burned down a lot is, I think, in a utopian construct in the future is if you had an air force deployed a naval force, a ground force, and a space force all out there.

When everything is geo registered, so every weapon is known. It's known exactly where it's at. It's known exactly what it can do, and what type it is very similar to call of duty. You can tell exactly what weapon you need in a different scenario, and when a system, whether it's aerospace detects a long range target, you use AI, ML and it does very similar to facial recognition. It can go based on its characteristics, detects this threat. I know what its vulnerabilities are. I know the optimal weapon against that kind of target, and vulnerabilities, this type of weapon. It knows where the weapon is, and when you can order the weapon, like you order an Uber, you're halfway there.

And, you go, "I need this." And, it goes, "Roger." This is the weapon, this is the place, and then, when the weapon is actually released by, now this gets to the human. Who commands and controls that to be allowed is a human discussion, and a decision. Once the weapon is released, when we've crowdsourced everything, so we know where every threat is, we understand what it looks like, and the weapon can navigate the threat lay down very similar to how we would navigate using ways to understand where all those threats are. You're kind of the rest of the way there, so the system is now all interconnected of ordering the weapons, having it navigate.

And then, the hard element is really that human element of command and control, of who is making the decision, because I think, we're going to be some ways off before... You want machines making life and death decision.

Lee Hutchinson: That was going to be my next question. I have a couple more here, and I don't mean to go all philosophical and stray off here, but that's something that we will eventually have to run into. I don't think you'd find anybody in like our generations, and I think I'm 42. After 40 it gets hard to pay attention, but I don't think you'd find anybody who is currently sort of an adult and alive today who

would be super duper comfortable with releasing battlefield decisions like that completely into the hands of an algorithm, especially, knowing how bad some algorithms are, and how dumb some of the search results that we all get are sometimes.

But, this will become a question in the near future, not necessarily in the next maybe five years, or 10 years, or whatever.

PART 3 OF 4 ENDS [00:24:04]

Lee Hutchinson: ... future, right? Not necessarily in the next maybe five years or 10 years or whatever, but we're going to eventually get to where we will need to think about that, right?

Scott Stapp: It depends because there's two pieces of this. There's the offense piece and the defense piece, right? So if somebody is salvoing in large numbers of weapons into your platoon's area, you want to go defensive and it's just too many things coming in, you may not have a problem putting it in auto mode to start throwing things up because it's really protecting you and it's not harming anyone else. It's really trying to destroy things that are coming in. I think doing that will give us a lot of the learning curve on how effective those algorithms really work. Do they do what they're told? How often do they deviate? But it's less of a life and death situation.

I think the only time we're going to be looking at it in an offensive fashion, like we might do that offensively. So here's what's funny, if you think about it, if you launch a surface to surface weapon system, from the time you push the button and it launches, you really don't have control of it anymore. It's really autonomous anyways. Right? It's ideally going to its GPS coordinates. It's doing those kinds of things. Right? So there's no recalling it. It's the first step towards its doing it by itself. I think they're going to have to think about through, there are a ton of moral issues and discussions around letting it just operate on its own. I think the DOD is going to be extremely reticent to what we'd call man on the loop rather than completely out of the loop. Right? I think you may see either the man in the loop or the man on the loop verifying that the decisions are correct so that it can stop it at any point.

Because, and again, our adversaries, I'll be honest, I don't think our adversaries are going to have the same moral dilemma that we do in the United States as a country. The value of human life in the US and with our allies is much higher than a large portion of the rest of the world. And so, whether it's our lives or our adversaries, we have this value of human life that they just don't want, we always are concerned about collateral damage or concerned about those effects. That is not the intent. We have a law of armed conflict. We have rules. The idea is never to get into a conflict. But when you do, there are rules to it, which is minimize human casualty.

Lee Hutchinson: Yeah. And you definitely wouldn't want a weapon system making a choice to take a life unless that choice has already been sort of approved. Right? You wouldn't want your weapon system, I guess, defining your rules of engagement, only operating within them.

Scott Stapp: I think that is exactly right. And I think we will be so far off on getting everything connected and having AIML, as we learned that as we get to that point, we will either have more confidence in what it can do. And again, I think it's very similar to the internet of things. I think folks who were doing internet banking and trading and actually working in the medical community, probably had some reticence to start with. And if you look at it, the medical community has done amazing things in AIML, when it can look at x-rays and ultrasounds and it can do cancer detection at significantly higher rates than a doctor can. And it just took them time to get there. Right? So a lot of this is exposure, it's trust.

So what you get with humans in any scenario, especially in the military, is with teams working together, they develop a sense of trust. If I do this, I know my fellow commander is going to do Y. It's just the sense of trust. The more they work with AI algorithms, and we have this interconnect of things, the more the machine does exactly what we expect, the more trust we will develop and the more likely it will be to be used.

Lee Hutchinson: Sort of a logistical question. I know you've heard the old saw about how there's really no such thing as the cloud. It's always just somebody else's computer. And when we're talking specifically about this idea of the integrated battlespace, where are these servers, right? Is this units are bringing computing power with them? Or as you establish like a forward operating base, is there a little server farm in a hardened box that they stand up? Or is all of this being transmitted and all the computation stuff occurring offsite, like speech recognition on your phone?

Scott Stapp: I think you're going to have a combination of both. Ideally what you would like is you would like those server farms. You're right. It's always just somebody else's computer and they're dispersed, or they're in large warehouses with 50,000 servers. There's always going to be some need for reach-back. But in some cases, reach-back causes latency. And in any rapidly moving battlefield, latency is not good. So you will find that we will have upfront what we call edge computing, and they will either take them with you, which is why Moore's law is, we're hoping it's continuing and continuing because you get more storage and processing power in smaller packages.

So if you can take an aircraft that you use for, you will say a bomber, right? If you have a bomber that normally has that mission, but you decide, "You know what? I'm not going to pack this one with bombs. I'm going to pack it with edge computing. I'm going to have that be my airborne node that actually does data storage, data computation, and has comm links that helps share it with everybody else." We're going to be looking at those edge computing and you're going to see it. It's going to be done in space. You'll have edge computing in

space. You'll have it in air. You'll have it on ships. You'll have it in a ground systems with both the army and the Marines. And you can't have everything. But what you want is you want those critical elements where latency is your biggest problem. And then in other cases, you will have reach-back to other elements that may be looking for historical information or updates or other things, but things that are not critical that they need in immediate nanoseconds.

Lee Hutchinson: Do you see a lot of this happening with perhaps commodity consumer type hardware that's been slightly modified for battlefield use? Or do you see a lot of this happening with customized, ruggedized stuff with custom silicone or whatever?

Scott Stapp: You're seeing a lot of this, I think, is going to end up being in custom processors, some level of custom storage. But as you see silicon and CMOs with what they call these advanced nodes get smaller below 10 nanometers, you're going to see an ability to customize both on the processing side and the storage side for what you need for that specific mission.

Lee Hutchinson: That's fascinating. That's neat stuff. Scott Stapp, thank you for taking the time to talk with us. Really appreciate you coming by.

Scott Stapp: Thank you very much for having me, Lee. I really appreciate it.

Lee Hutchinson: Absolutely.

That was Northrop Grumman chief technology officer Scott Stapp on the internet of military thing. Come back next time for the second part of this special edition of the ARS Technicast, where we'll talk with Northrop Grumman vice president Richard Sullivan about the role of open and secure systems in this new vision of the modern battlefield. Catch you then.

PART 4 OF 4 ENDS [00:31:08]