Mike Wynne, Former SECAF
General Hawk Carlisle, Commander, PACAF
General Mike Hostage, Commander, ACC
Maj Gen Linda Urrutia-Varhall
David Fahrenkrug, Author
"21st Century Warfare: The Combat Cloud"
AFA - Air & Space Conference and Technology Exposition
15 September 2014

Moderator: Good afternoon, welcome. As David said, I'm David Fahrenkrug and I was asked a few months ago by General Deptula in the Mitchell Institute to take lead on writing a paper about combat cloud. It's a concept probably some of you have heard about, seen or put on a piece of paper. You maybe even wandered in this room just because you're interested in what the combat cloud is. But this panel is actually part of a much broader project, and the project is going to go on after this. General Deptula is going to continue the study on the combat cloud, but the combat cloud is meant to address changes that we see happening with 21st Century warfare, specifically changes that are occurring because of the way we are deploying and using information systems and the way we've been able to access information. But significantly, the fact that there are other people who are trying to deny us access to that. So truly in a sense that this is combat, we have an adversary and we're going to be engaged in a competition over who controls information.

No doubt many of you wandered into this room just to figure out what the combat cloud is, and I'm going to give you some brief remarks about that and then I'm going to look to our panelists to help flesh out a couple of these ideas.

I suspect that everyone in here walked in this room connected to a network. In fact, that connection is going to allow you to do many incredible things. If you wanted to know what the weather's going to be in 15 minutes or 15 hours you could look that up instantly. If you were getting bored and wanted to multi-task and buy some stock with Apple, you could do that while you're listening to me. If you were wanting to verify some of the facts that this panel is going to put forth, you could Google that and know the answer before we finished talking. This is the reality of the world we live in from an informational society perspective.

But this is not the reality we live in when it comes to combat operations. In fact, despite the fact that technology is obviously changing the way we live, the way we wage war has not changed so obviously. Just as World War I was fought with 20th Century mechanized forces using 19th Century practices, we are in danger of going into 21st Century warfare fighting with 20th Century practices. We have informationalized equipment that should allow us to fight a war in fundamentally different ways.

To truly take advantage of the Information Revolution, U.S. forces will need to not only adopt new means for waging war, but also develop new ways for using and targeting information systems. The networks are going to war and information is going to be the key resource that we are going to need to gain control over in any future conflict. In fact the control of information will become as decisive as targeting any kind of physical destruction. Sun Tzu wrote about this more than 2500 years ago, but today we actually have fielded systems and have capabilities to make that a reality.

Other countries are seeing this as well. China has doctrinally determined that information superiority is the prerequisite to win any future conflict. And even though they are a decade behind the United States in achieving this operational objective, they are determined to surpass us and win the battle for information.

While we had made great strides in building an informationized force, the disparate number of networks -- SADL, MADL, IFDL, Link 16, Link 14 -- and the vast number of concepts -- Joint Information Environment, JALN, CEC -- means that we have not yet crossed the threshold to fully taking advantage of our informationized forces.

As we speak, the Marines are running around the desert in Yuma, Arizona desperately trying to figure out how to incorporate the F-35 into the MAGTAF, and I'm sure they're going to figure it out. The F-35 is being fielded with an incompatible network that cannot even share information with our other fifth-generation aircraft. This is not a war-winning strategy.

The Combat Cloud - 9/15/14

So the combat cloud and the project that General Deptula is leading up, is to find our war-winning strategy. So the panel today is going to help illuminate some of the concepts behind how we're going to win the war. How we're going to win the next war using our informationized systems.

So with that rather somber assessment I'm going to now turn to panelists. The way we're going to proceed from here is, I have a question that we're going to start off for them each on their opening remarks. Secretary Wynne, I'm going to begin with you. Simply, what are your thoughts on how the Air Force is postured to take advantage of the ongoing Information Revolution and what do you think are some of the top challenges we need to address?

Secretary Wynne: David, thank you for that somber assessment, and thanks to the Mitchel Institute and the Air Force Association for having me today.

The combat cloud cries out for definition in an operational concept. When you say combat cloud it is reminiscent of the Tower of Babel where according to the best record, "Though each spoke in very disparate languages, all could hear in their own language." When you infer an operational concept from that it requires a pre-definition of receipt and transmission from the best frequency-hopping software controlled radios, and a set of icons that are a universal subset of the combat fighting forces.

This operational concept also requires that if Aegis or ground-launched missile such as Patriot or [GLMRS] participate in the combat operation which we're beginning to expect as expressed in the notional Aegis as my wingman from the naval proceedings and the Army commander in PACOM who recognizes the forward role that the Army can play in defense of the Pacific as was written in an interview with the SLDInfo.com folks.

So this notion of active targeting, selective shooting, and sharing of situation awareness is now in play in the minds of warfighters, but the question of can it be a war-winning strategy is a part of the somber assessment. We need to reenergize Red Flag and joint exercises to both vet and test concepts of operation.

The Combat Cloud - 9/15/14

The emergence of the F-35 is completely rewriting the U.S.
Marine Corps' approach to tactical and from the sea engagements
and will for each of the air forces that recognize it not as
replacement fighter but as a brand new approach to offensive
battle management. Its role and the role of the coming long
range strike in the combat cloud can then be seen as central.
As many coalition partners will also be F-35 operators this
extends the reach of the cloud into international territory.

I have postulated that America must rethink force structure to
consider offensive enterprises and defensive enterprises. And
the roles that remain available for fifth-generation, legacy
assets, and unmanned or remotely piloted systems. The reason
for this is the concept of operations is altered dramatically
for JSTARS, for an AWACS-like, and for fifth-generation
aircraft.

Many of you have heard my concern that the F-22 is the best
collection system on the planet, but only advises the pilot of
the situation report. This has to change. The system is
working on it, but for now it looks to me that the lead in the
defensive enterprise as there will be other systems to monitor
and guide supporting aircraft to defeat and deter an aggressive
enemy.

If you have followed my writings you also read that I don't
think JSTARS or AWACS will survive for long in an anti-access
environment or a close air fight. This means 200 miles at
present. That said, they will do terrific embedded in the
defensive enterprise given their long view and the ability to
guide forces to gaps.

Also, this enterprise is very useful in permissive environments
such as where they're in use now. With the present state of
lethality we seem to shy away from anti-access systems even with
our finest fourth-generation fighters. This means that with our
F-35 or F-22 we can anticipate lethal response to any bombing,
missile firing or gun shooting in a well defended zone.
Therefore we need to consider a few changes in our approach to
the offensive enterprise.

The Combat Cloud - 9/15/14

The F-22 or F-35 exercising their target find capabilities needs to identify and export the target data to any available shooters other than themselves. This is the historic role of the artillery forward observer, the infantry scout and the Navy coast watchers. Available shooters must sit outside of the lethal zone which we refer to as the forward edge of the battle space or in the case of unmanned or remotely piloted vehicles, fly in the vicinity but nowhere near the fifth-gen airplanes.

Once receipt of targets are recorded, the shooters need to commence firing and create a gap for penetration and hopefully take down any approaching enemy aviation assets.

When do the fifth-generation fire their weapons? As a last resort in an offense and as a first resort in defense. Frankly, in the stealth mode they simply don't have enough weapons and need other shooters to initiate the engagement, but they can blunt any attack force and make the enemies very uncomfortable.

I wanted to go to this depth such that the operational concept of combat cloud can be fleshed out, developed, and really tested. We will need all of our Air Force assets and those of our coalition air and naval forces. Many will be called and they better be sorted into useful fighting and logistical forces.

Thanks for listening. Back to you, Dave.

Moderator: Thank you, Mr. Secretary.

General Hostage, over the course of your career what are the top two or three changes you have witnessed in the employment of air power, especially with regard to the use of information technology?

General Hostage: Thanks, Dave. I appreciate the opportunity to be here today. Top two things. It's hard to come up with a list of just top two.

Let me say, I flew my first fighter sortie in a Block 5 F-16 and on a good day you might see 12 to 17 miles. If you see an Eagle

at 17 miles you're a happy camper. You're dead, but a happy
camper. [Laughter].

I flew my last fighter sortie in a Block 3.1 F-22 and I think
that will probably give you the answer.

In my F-16 I had an inertial system that was good for about 20
minutes before I needed update it. It was good to a half a mile
for a full mission, but if I wanted to hit a target or something
I needed to keep updating, and once you started you just had to
keep updating.

The Raptor, the ubiquitous GPS. Everybody's got them. I've got
them in my pocket on the phone, I had it in the airplane, I mean
we all have them.

Datalinks, what I learned flying the F-22 is all of the mundane
things that a block fourth-generation aviator worries about --
communicating position and status and such, that's all in -- the
machines do that. In a well-briefed mission in the F-22, the
two Raptor drivers never talk to each other. All the
information they would normally be passing back and forth is all
displayed by the system. They're doing a much higher level of
battle operation than the fourth-gen aviator.

So in my view the fusion capacity of the fifth-gen is really,
that's the defining characteristic of fifth-generation. It's
not stealth. Stealth is one of those things that came along
with fifth-generation but the fusion is the most important part.

That gets us to the linkage to the combat cloud. Right now our
fusion, as the Secretary rightly pointed out, is all inside the
engine, the computing engine inside of the Raptor and it will
share it with other Raptors, but it isn't able to share with
anybody else unless the pilot gets on the radio and starts
transmitting it.

The F-35's going to come along and share very well with its
partners. It's not going to share a lot with everybody else.

There is Link 16. We're working Link 16 solutions, but one of
the most critical things I'm pushing our 5-8-9 folks to get form

industry is a fourth to fifth/fifth to fourth solution because I need to leverage all of the fusion capacity on board the fifth-gen to help the fourth-gen.

But even at that point I'm just linking tactical platforms to tactical platforms.

The next thing is how do I pull national data out? How do I pull the command data from the AOC board? I can do that in single links but those links are vulnerable. So the concept of the cloud, the combat cloud, it's just the same cloud that we talk about in our private lives today using the internet and the cloud. It's data that just lives out there, it's constantly updated, its constantly fresh, it is ubiquitously available anywhere, anytime, no matter where I am.

The combat cloud is probably not going to be as pervasive as the commercial cloud, but what I need is in the battle space the ability to tap that larger reservoir of information and know I need to have certainty of data. I need to have availability of data. The combat cloud won't reside on a single platform that if taken out or it has to go to the tanker all of a sudden all the information is lost, which is the challenge with especially those tactical links is if you break the link chain, you've reduced its capacity. The combat cloud needs to be out there, it needs to be gracefully degradable. If one of the links has to go for gas or breaks or falls out there is still a cloud out there. It may not have all the connectivity it had before but it's still out there and it's in the immediate battle space.

In the worst case scenario, the A2AD environment where a command element is cut off, the AOC is cut off from the forward edge, I've got distributed control nodes out there -- my VMC2 platform, JSTARS is out there, I've got AWACS out there. I potentially have a wing operation center out there in the battle. Somewhere where I can have that distributed control still functioning, populating the combat cloud. You just tap into the combat cloud providing the information to the battle space where the tactical players can have access to ready and current information.

It's been a world of change from the start, but I would never want to go back to those old days.

Over to you, Dave.

Moderator: Thank you, sir.

General Carlisle, you're coming from a slightly different perspective than the rest of the panel in that you were staring across the water at a potential adversary and one, as I mentioned earlier, who has identified this as a key area of competition in the future. So I'd be interested in if there's a potential conflict in the Asia Pacific how do you see the view of the future of air power given the increasing use and dependence on information system?

General Carlisle: Thanks, David, I appreciate the opportunity to be here. Thanks for inviting me. I have to admit that I am a well-known and self-admitted techno-peasant so the fact that you invited me to be on this panel is a little bit shocking to me. Mike made the comment when I walked in, around me it's the cloud of confusion, not the combat cloud. [Laughter]. But it's great to be here.

I think we're facing some huge challenges and I'll kind of address those for a second, then some of the things we're looking at and what Mike and I have been talking about for the past two years of how we're going to move this forward.

In the AOR that I face, the first and foremost thing that I think a lot of people fail to realize is distance and the paucity of satellites, land bases. Everyone's heard the numbers. There's 60 percent of the world's population; 52 percent of the earth's surface; on 17 percent of the earth's land mass. Which tells you density of population and the lack of satellite coverage, the lack of land-basing capability.

The example is, people talk UAVs, and you need a UAV in the Pacific that doesn't have 300-mile combat radius, it has to have a 1,000-mile combat radius because that's what it needs to deal with those kinds of distances.

That also causes, when you talk about a nodal system and the ability to maintain that big data and that information network self-healing combat cloud architecture type thing, you have to be able to do that over thousands of miles, not hundreds of miles, and that's a huge challenge.

The second challenge we face in the AOR to air power is clearly the threat. The pacing threat that we face today is what the PRC can generate and how we react to that. If you look across, and we spent a lot of time and there are some great studies going on reference the EW spectrum and where the PRC is covered, and they cover the spectrum. You look at every single platform and system they have and their ability to counter us in an EW spectrum which is part of the A2AD environment. It's the anti-ship ballistic missiles, it's cruise missiles, it's the ballistic missiles, and it's also their EW capability. And that, when you talk about combat cloud and your ability to operate in that environment, that's one that again has to be part of this discussion as we move forward.

The final one is, we're not going to do anything alone anywhere in the world, and I guarantee you we'll never do anything alone in the Asia Pacific, Indo Asia Pacific. If something happens in Northeast Asia, the Japanese are part of it. Period. Dot. So whatever we do has got to be inclusive of the coalition. The Australians, the Koreans, the Philippines. Every one of those places has to be part of it. Do they have to be a full player? Or how that works in the case of maybe the Philippines, but they have to have access and they have to be able to operate in that. In the case of the Australians and the Japanese, we have to be at the high end. They have to be basically full-time players across the spectrum, and we see that today as we do information sharing and data sharing.

In some of the work we've done with the Japanese recently, we've moved significantly down the road with respect to information sharing, but we have to build that into the network. It's got to be baked in from the beginning. It can't be brought on afterwards.

So as Mike was saying, we've spent a lot of time, and one of our lines of operation in the Pacific is agile, flexible C2 in a

contested, denied and disrupted environment. So our ability to
do what Mike talked about, centralized command, distributed
control and decentralized execution and how you execute that and
what you're able to do. That is dependent upon not only cloud
technology but network technology, network collaboration,
teaming between manned and unmanned systems. And today we can't
-- we're working on it. We've got a long ways to go but we've
been working on it for a while. We can't even build the right
plumbing that we all agree to. The Navy and the Air Force
aren't necessarily on the same sheet of music when it comes to
network collaboration and advanced tactical datalinks. Again,
we're working on it but the Navy with NIFCA-CA and the TTNT and
where they're headed; the Air Force in an LPI/LPD mindset with
MADL and IFDL, and then the network connectivity through
gateways, whatever those are in the future, it's going to be a
way of the future but we've got to think about how we get to the
next level and we're not there yet.

The biggest challenge, to answer your question is, we've got to
get that understanding of what that network collaboration looks
like, what the advanced tactical datalink looks like, what the
combat cloud looks like, and how you do C2 in a contested,
denied and disrupted environment.

And the challenges we face are the vulnerabilities that exist to
all of them. And it can be natural disasters or it can be
distance. Most folks probably know that after the great east
Japan earthquake and tsunami, the Korean Peninsula was cut off
for a period of time. It had nothing to do with adversary work,
it had to do with a natural disaster that occurred off the coast
of Japan and broke all the fiber cables and the HTAC at Osan was
disconnected from everybody. Those are things that have to be
part of the discussion as we go forward.

The other one, and I have to tell you this is one of the most
frustrating things we see and I think everybody's frustrated
with it, but we need industry to help us is, Moore's Law versus
our acquisition cycle. So Moore's Law says every 18 months
information technology changes and it takes us six years to
acquire something. So by the time we acquire it it's four times
out of date. And you just can't stay not -- You can't prevent
vulnerability when you have to equate those two together.

Finally I think, and we're working on it. Again, we've got a long ways to go. But centralized command, distributed control and decentralized execution, we've got to start thinking of the ConOps. What does this look like? There's a lot of great technology and DARPA and some of those folks are doing some great work on what the plumbing looks like what the data packages that are passed like. You need to know what you need to know, when you need to know it, and nothing more because you can't digest it all. But we have to get to the ConOps as we move forward.

So those are the challenges I see we face in the Pacific AOR. Thanks, Dave, and again, I appreciate the opportunity to be part of the panel. Thanks.

Moderator: Thanks, General Carlisle.

I don't think the news is getting any better.

General UV, in your unique position of overseeing a lot of the systems we've been talking about, if you could provide us some insights about how we're going to be able to adapt to some profound changes we've already seen occurring with the way surveillance and reconnaissance assets are used, but also how intelligence is going to be collected, processed and distributed in this common environment.

Maj Gen Urrutia-Varhall: David, first of all thank you for inviting me to this austere panel with the former Secretary and two four-star generals. Boy, am I lucky today.

But Air Force intelligence, surveillance, reconnaissance, or ISR, is at a strategic turning point. In a world of increased strategic uncertainty where threats continue to arise quickly from multiple locations, our network of Airmen must seamlessly integrate and fuse information from all sources across the air, space and cyber domains, as well as operate a mix of sensors across the entire spectrum of conflict. This includes operating in an anti-access area denial or a highly contested environment.

The Combat Cloud - 9/15/14

Currently we process, exploit and disseminate by platform with analysts watching a full motion video feed -- now in full color as opposed to 2001 when it was black and white; and also in high def when in 2001 it was grainy, poor quality; and direct reporting to our forward forces. The high data volumes with broad area persistence includes signals intelligence plus radar, visual, infrared imagery integration, overhead persistent infrared layers, and yes, open source which has become a valuable player. I would have never thought 30 years ago that open source would be an intelligence platform that we would use as much as we do today.

However, all this data coming in comes in with huge challenges. Air Force units today have approximately 1600 hours of video per day. That's right. Let me give you an equation. That's equivalent to two NFL regular seasons -- a day.

With our complex security situation not looking any better in the future, RAND estimates by 2016 -- two years -- we will need over 100,000 people to process, exploit and disseminate with today's processes and tools.

So this leads to the requirement for automated correlation of fusion tools and a refocus on analytical methodologies and trade craft. In the future our mix of sensors and capabilities we employ to execute global integrated ISR will change as we prepare for operations in anti-access area denial environments.

Our Air Force ISR enterprise must be trained and embrace the technology combat cloud offers us to operate across the spectrum of conflict. ISR in contested environments challenges us to use sensors from all domains to collect the right information at the right time. Within analysis on the technological side Air Force ISR professionals need a robust and secure data cloud with information and data tagged for ease of retrieval and used by analysts regardless of the platform.

Additionally, we have to grow world class expertise across a spectrum as an integral part of air component and joint operations. It requires Airmen who are masters of threat characterization, analysis, collection, targeting and operations intelligence integration.

ISR 2023 Strategic Vision is a globe of sensors and platforms
producing data that is processed and conditioned into an
information cloud. Additionally, the volume of information
streamlined using cloud technology can be manipulated by a
distributed enterprise of multi and all source analysts; layered
missions and organizations such as squadrons and wings; air
operation centers; and intelligence-producing centers; in synch
with the other services national data analysis nodes to include
law enforcement which is becoming bigger and bigger in what we
do for the overall national data set, to produce decision
advantage, multi-aid analysis, cross-cue and fused across
SIGINT, GEOINT, HUMINT, and yes, open source.

This information cloud needs to be an adaptable, robust, agile
and globally distributed network. Seamless, multi-security,
open framework that is enabled by cloud technology, embraces any
domain, any sensor, any data, and is interoperable across air,
space and cyber. Such an open architecture will better enable
us to respond to crises globally.

Now is the time to approach technology with an out of the box
mentality to preserve our advantage.

To us, Benghazi is a new norm. Back in September 12 when we were
at the U.S. Consulate in Libya it took us 30 days to respond
with a remotely piloted aircraft CAP.

Let's fast-forward it to July when we were against ISIS in
Baghdad. It took us 24 hours. That's right, 30 days to 24
hours to respond to the ISIS Threat with an RPA CAP and
actionable intelligence. That's the benchmark for ISR and
command and control. Strategic agility.

With that all being said, even with the increased data, ISR is
still not meeting and probably never will fill the ever-
increasing ISR appetite of the COCOMS. We have to shift from
demand-based to supply-based model. The future needs to be
configured to provide dynamic presence and global agility that
allows coverages of area of responsibilities and concern with
fewer locations and assets.

The Combat Cloud - 9/15/14

We have to be able to provide better coverage, faster response to crisis, shift weight of effort from theater to theater based on maybe weather, priority and crisis. And along with meta-tagging data and using all data available including data not initially exploited, big data analytical applications such as activity-based intel (ABI) or object-based production will allow our analysts to discover the unknown unknowns and satisfy commander requirements or needs not yet formulated.

Additionally, we need to provide a push environment for dissemination that will allow real-time tactical advantages for all our operators.

Thank you.

Moderator: Thank you, General UV.

Before I throw the mike out to the audience to let you have a go at the panelists I'd like to just kind of summarize succinctly here on a couple of points I think all four of you have brought up. And if I may, in general you have given us a little more insight into the problem. So I think as an audience we have a good sense that there's something that needs to be fixed. And General UV, you concluded by giving us a couple of things as far as big data analysis and demand-based, fly-based, meta-tagging, the kinds of things we've become comfortable with in our private lives that we have available to us but haven't been so in combat operations.

Both General Hostage and General Carlisle, you mentioned this idea that not only do we need plug and play capabilities that we can operate with our allies, within our force structures, across the services, but General Carlisle you mentioned even the further requirement about how we're going to do spectrum control and the idea that our networks are dependent upon how we actually manage our spectrum.

Finally, Secretary Wynne, you started off with probably one of the hardest things, and that is what's our concept? What's our operational concept? Then how are we going to train to that operational concept?

So that sounds like a pretty challenging problem that we're going to need to overcome. So what I'd like to throw out to the panel, and I'm not sure if we have time to get through all four of you, but I would like to talk about one thing that we should be doing. One of the things we struggled with the combat cloud project is, what do we do about this? As commanders who have the ability to cause things to happen, what are some things that we should cause to happen?

Secretary Wynne: Dave, let me start, then I can get criticized. That's the best thing.

This is going to start at the very tactical level, at the very lowest level of tactical engagement, and we're going to notice that these young aviators are going to change the way that they do business and pass it up, hopefully, to group, wing, and commander. So I believe that we are far from having an issue, we just need to authorize them, if you will, to play. And when they do play we will find that they have invented a new way to pass appropriate information and that we should write down.

General Carlisle: One of the things I Think we need to figure out how to do in a lot of this has to do with some of our FFRDCs and [Omiters] here and other ones, as well as our industry partners is the Moore's Law versus acquisition time line. We have got to figure out how to do open architecture, the ability to spiral into things so that we don't have to worry about the cost of doing OFP changes for a new wave form based on a threat that has changed the way that he's going to attack our ability to do network and ConOps. So I think that -- And that's not easy to do. We've been thinking about it for a long time. But the idea that we can do an open architecture or that the technology gets us to the point that the systems don't necessarily care about the wave form because they can talk in any of them. It's the Tower of Babel concept that Secretary Wynne mentioned.

So I think, and we're doing some great work. I think the idea of understanding the plumbing and then within the plumbing to allow that network collaboration and teaming, then how you pass data and what the requirements are for that data. The systems engineering that goes with that so that you have that open

architecture and ability to spiral or adapt inside of -- It's almost like in a tactical fight you have to be inside the adversary's decision cycle. This is exactly the same. You have to be inside their ability to counter [you] cycle and that's what that's going to require.

General Hostage: I think Secretary Wynne said it, it's going to start at a tactical level. The near term immediate solution is I need to link fifth to fourth, fourth to fifth, and if I've got to start just by linking fifth to fifth, that's a positive thing. If I can just get information from the fifth to the fourth, I'd love to get it back the other way, and I've already got some of it with Link 16.

Hawk's talked about the acquisition cycle. What I can't really stand is solving the problem with our standard six year cycle to produce something that's four generations of technology out of date.

So start with the near term, get those linkages, and my belief is you have legacy, you're going to live with legacy, so you start with how do you bandaid the legacies together so that they're talking. Then you can figure what the elegant solution is in the future and work your way towards that as you bring new systems in and don't make the mistakes of the past. IFDL to MADL all talking only to themselves.

But you've got to start with the legacy, make the legacy work because we're going to live with that for a long time. We've invested in it. That's the nearest term way to get to a solution.

Maj Gen Urrutia-Varhall: Just real quick.

For right now I'd argue for counter-terrorism that we find, fix, finish very well. What I'd like to do is work with industry so we can leverage technology and enhance analyst tradecraft so that ISR can be proactive instead of reactive. We need to answer the questions before they're even asked.

Moderator: From our audience, and this is somewhat related to what we were just talking about but I think they're trying to

get a little more specific. How do you incentivize future weapons and C2 developers that in order to play in the environment they must plug into this combat cloud at delivery? Then how do we hold them accountable to deliver as required?

General Hostage: Hawk already talked about it. It's open system architecture. We're trying to drive the Raptor to open system architecture as we move to the next hardware builds on the airplane.

I think it's converting the business model that we kind of grew up with which is a proprietary solution with proprietary hardware which requires proprietary contracts for service and support over time, to what the internet has already figured out is how to make money in an internet-based or an IP-based world where you hang a solution out there and the viability of your market is how many people sign up to use that solution.

Again, we have to provide the architecture which is, the corollary is the internet. The corollary is the combat cloud, and hang within that cloud different solutions. Then anybody who can build the better mousetrap can bring it to the cloud and it will wind up getting used because that's the best way to get business.

But breaking away from the proprietary business model to an open architecture to an internet-type app, download an app type mentality, you guys have to, industry's got to figure out that business model and get comfortable with it and then figure out how to compete with it. We've got to drive ourselves and our industry partners to an architecture that supports it and I think we'll be in an area to start beating up on Moore's Law and the acquisition cycle.

Moderator: I'm going to synthesize a few of the cards here. Following General Hostage, sort of that thought about changing our focus, changing how we approach the problem solution. One of the outcomes of the combat cloud working group is the idea that we have grown up in a highly platform centric kind of way of life. Programs are developed based off of platforms. The information systems that go onto those platforms are focused on the platform. Rather than if this is truly an information

battlefield then where is the focus on how information systems are fielded? And how are information systems fielded and put onto different types of platforms made available in different ways.

So a question that came in, this is for General Carlisle but I think is applicable for the whole panel. If we can agree on datalinks and networks to enable the combat cloud, so if we're going to field some type of network architecture, that's going across an enormous number of stakeholders not only within the Air Force but across all of OSD. We're going to field capabilities. We'll just focus on that. How is the Air Force going to tackle this problem? Who's in charge of the combat cloud information? Which phone number would I call?

General Carlisle: Well for about another two months, him. [Laughter]. Then after him, me.

When you think about it, as the owner of the C2 for the Air Force, certainly the core function, it's ACC.

I think your point's well taken and Mike is exactly right. We're working at it fifth to fourth, fourth to fifth, translators, there's some programs out there that are moving us down that road because we're going to be with the systems we have today. When we fight in ISIS tonight, which we're doing, sitting on the Korean Peninsula today, we are dealing with what we have and you have to have those translators.

The belief and hope is that, as Mike said when we get to the exquisite solution, is that you'll have, it will actually be wave form potentially agnostic and the systems will be able to translate themselves. So you drive, again that goes into the open architecture. Then if you've got the plumbing figured out of how it's transmitted and then the information packets. If you have born in translators to whatever you're dealing with and at the same time you would have to have some multi-level security type of capability. So again, you pass the data you want to pass. Nothing more. Then again, protect against vulnerabilities. But that's the exquisite solution down the road and where we're going to. But in the C2 core function, you're kind of looking at them.

Secretary Wynne: For industry that's out here I would suggest that you take to heart the not changing the OFP. And I would suggest that somehow you design a buffering system that takes on board all the various inputs and converts it into a similar to standard signal interface. So that the plane believes it's getting the data from its onboard sensors. I can tell you that you've got to think hard about how to separate it. The reason you've got to think hard about separating it is the way we do acquisition and procurement now is if you alter the OFP it is a huge deal and will take months if not years of testing to prove that it didn't cause a dilemma for the pilot or the blue screen of death.

So if you think about it, that means you've got to go external and yet provide to that system something it already understands that you can convince the testers is the same as the signal processor that's already on board.

Moderator: Thank you, Secretary Wynne. We are at the end of our time. So let me just wrap up very quickly.

First of all, thank you. Thank you for sharing your experience and your insights. This, as I said at the beginning, this is a bigger project and it's a bigger problem that's not going away. For two reasons. One, we're still fielding incompatible systems and we have an adversary who likes that.

So we have solutions that we need to pursue. The Mitchel Institute is committed to putting out a vision for how to go forward with the combat cloud and how this is going to affect the way U.S. forces operate. So I anticipate seeing that coming that coming out in the next year as General Deptula leaps forward with trying to put out this vision for where we go with future combat.

Thank you all very much.

                              # # # #