THE COMBAT CLOUD: A VISION OF 21ST CENTURY WARFARE

Keynote Address

Lt Gen David A. Deptula, USAF (Ret.) at Association of Old Crows: Dec 1, 2015: Washington, D.C.
General Deptula is the Dean, Mitchell Institute of Airpower Studies.

Good afternoon ladies and gentlemen, and thanks for that kind introduction. It's a privilege and a pleasure to be here today to address the group of people who have the knowledge, insight, and common appreciation for the value of electromagnetic spectrum operations as a critical element of national security.

I'd like to open my remarks this afternoon with a scenario set in a high intensity conflict sometime in the future. In the opening phase, a Marine Air-Ground Task Force is escorted by F-35Bs. It's conducting a raid against enemy anti-ship batteries to enable insertion of friendly forces.
Upon reaching the objective, a SOF V-22s is downed by the enemy. The raid continues and help is sent to extract the injured. As enemy air defenses begin to react, F-22s target two surface-to-air missile sites and team with F-35s to further suppress other threats.

The situational awareness tools are common across all platforms in the force. The F-22s and V-22s are able to detect, then federate the detection of threats so that the force's limited weapons are employed against the priority threats.

The F-35s tap into the same picture, populate with other data, and broadcast the status of the threats. Both SOF and general-purpose forces in this raid have an accurate picture of the opponent's defenses sensed by the friendly aircraft.

In the secure video debrief conducted five hours later, the strike commander credits his ability to see through the confusion caused by the enemy response as the reason the strike met its attack objectives.

He adds that while 3 people died in the MV-22 crash, none were lost during the actual attacks against the enemy missile batteries. Injured personnel were evacuated; other losses avoided, and new attacks formulated by the real-time data available to the ground strike team.

The F-35 and F-22 flight leads agreed that the real-time display of the status of opponent defenses; communications; and emissions allowed them to enhance their attack against relevant threat systems.

U.S. space operators observed that the stability of the command and control nets gave them the information they needed to alter the view of satellites that provided inputs to the F-22 / F-35 hunter-killer team.

The F-22 flight lead described how he leveraged four unmanned combat air vehicles assigned to them to improve jamming, and enhance their full motion video link to the Maritime Operations Center.

Lastly, cyber operators revealed they were forced to work through several challenges to network stability caused by enemy cyber forces.

So, what's different in this scenario from how we do business today? Clearly evident in the vignette is the sort of robust information connectivity that today is aspirational. Every player had access to high quality, high confidence data that let them peer through the fog of war to see what was needed to save lives; keep the attack moving; and orchestrate the follow-on actions to maximize success.

The problems of connectivity among platforms and the problem of connectivity among low RADAR cross-section aircraft operating deep within enemy space was overcome. In the final analysis, real-time data, enabled real-time decision-making, allowing every player to not only remain oriented in a highly confusing battle, but to reorient and out think and proactively shutdown the opponent's defense.

The force was enabled by a future vision of connectivity of every joint task force player instantly formed when in proximity to one another. However, this is not merely a recycled vision of net-centric warfare. It's a concept where every friendly force object and person is a component, router, and node in a real-time IP based constellation with low latency to enable accurate desired effects against priority targets.

You all will recognize immediately what will be required to actualize the effective operations postulated in the vignette, and what actions the enemy will be taking to deny our success...dominance in Joint Electromagnetic Spectrum Operations.

Electronic Warfare is integral to modern warfare and accordingly it offers a set of capabilities that can cripple an opponent's ability to sense, communicate, and exercise command and control within a battlespace—or do the same to us.

The U.S. Army's Foreign Military Studies Office assessed this year that Russia possesses "a growing EW capability, and the political and military leadership understand the importance" of such warfare. The assessment concluded, "Their growing ability to blind or disrupt digital communications might help level the playing field when fighting against a superior conventional foe."

Our US military leadership understands the same. In March of this year, DEPSECDEF Bob Work, acting on the conclusions of a recent Defense Science Board electronic warfare study, established an EW executive committee to address shortfalls especially in areas where EW and cyber are converging.

As so succinctly stated by Gen Israel, "The next war will likely be won by the side that best exploits all elements of the electromagnetic spectrum." So what must be accomplished to allow us to do that?

I'd like to focus today on the first step. I suggest that there needs to be a common vision that all in the defense community can understand, and accept as a desired way ahead. I'm not talking about a particular system, or acquisition, or service, or organization. We require the variety of separate and distinct capabilities inherent in our services, and other government security organizations that collectively make up our defense architecture.

However, we must be bound by a common appreciation for the value of electromagnetic spectrum operations as a critical element of national security. I am talking about a vision...a vision aptly described as still using elements of the well established notion of combined arms warfare, but moving beyond it to one of combined effects power. The kind of combined effects resident in a unified ISR, strike, maneuver, and sustainment complex integrated across the electromagnetic spectrum.

This vision is perhaps more descriptively labeled as a combat cloud. The concept has as its basis allied militaries linking information-age aerospace systems with cyber, sea, and land-based capabilities in ways that will enhance their combined effectiveness, while compensating for the vulnerabilities of each.

The combat cloud concept is somewhat analogous to "cloud computing," which is based on using networks to rapidly share information across a highly distributed system of systems.

However, instead of combining the computing power of multiple servers, a combat cloud will capitalize on the ubiquitous and seamless sharing of information among multi-domain weapon systems to rapidly exchange data between sensors and shooters to act as a cohesive whole.

If enabled by secure, jam and intrusion-proof connectivity, a combat cloud may be capable of employing fewer modern combat systems to achieve higher levels of effectiveness, across larger areas of influence, compared to legacy operational concepts. For example, instead of relying on traditional approaches that mass fighters, bombers, and supporting aircraft into major strike packages to attack particular targets, a combat cloud could integrate complementary capabilities into a single, combined "weapons system" to conduct disaggregated, distributed operations over an entire fluid operational area.

The combat cloud requires treating and equipping every platform as a sensor as well as a "shooter." It will require a command and control paradigm that enables automatic linking as does cell-phone technology today, and transfer of data seamlessly, and without need for human interaction within and/or between the combat cloud nodes, plus it must be reliable, secure, and jam proof.

While the overarching notion of actualizing a Combat Cloud with the degree of integration required to achieve a self-forming, self-healing, pervasive war winning complex is a new idea, many of the individual technological elements required to manifest this vision already exist or are under development.

But each was developed in the absence of an overarching, integrating vision. Examples include Link-16, IFDL, TTNT, MADL, and JALN. While delivering distinctive capabilities, the services developed each of these in a stand-alone manner without an overarching construct to ensure Joint and Allied partner interoperability, much less interdependency.

Establishing the Combat Cloud as the operational template for the various system linkages afford a basis of interoperability and more importantly, interdependency, to normalize existing systems; guide development on emerging programs; and establish common requirements. It would also highlight the critical relevance of Electronic Warfare to the realization of this vision.

Combat Cloud promises new operational effectiveness and efficiencies. Current systems are largely expected to operate in a semi-autonomous fashion, with a basic level of collaborative engagement with other platforms in the context of "jointness"—an organizational construct as that has yet to be fully realized.

These shortcomings place pressure on individual assets to possess numerous internal capabilities. The complexity inherent to this approach drives lengthy development cycles, which in turn leads to requirement creep, time and cost overruns, and delays in capability.

In sharp contrast, the Combat Cloud will enable individual platforms to harvest a wide range of capabilities by sharing critical information, thereby negating the need to possess all functions internally.

By affording numerous redundant function options through the Combat Cloud, individual platforms don't have to leverage as much from their internal attributes, nor do the services need to organize, train, and equip to operate "organically" to achieve self-sufficiency."

This represents a huge shift in how we prosecute war. Additionally, the Combat Cloud vision reduces the pressure to over-load requirements and allows individual platforms to evolve in a more cost-effective fashion.

The result is that individual systems are freer to strive to excel in specific areas. For its part, the Combat Cloud supplements a broader array of capabilities, and ultimately serves as a more effective and efficient means to achieve the intent of "jointness."

The same holds true for Allied interoperability. Partners around the world are modernizing their armed forces with new military capabilities that have the potential to enhance the effectiveness of a Combat Cloud-enabled force. Specific systems include F-35, Aegis equipped ships, P-8, Wedgetail, Eurohawk, and others.

Transforming these individual weapon systems into collaborative elements of an interdependent operational enterprise is what the Combat Cloud is all about. Whether discussing technical standards, common training standards, or established operational tactics, the potential afforded by individual Allied systems will only be realized if they are harnessed in an organized, deliberate fashion.

So let me describe the vision of the combat cloud a bit more. The physics of future combat platforms will likely not change significantly, but how these systems operate within future battle networks must change to realize the full potential of informationized warfare.

In order for combat forces to freely access and distribute information during combat operations, some existing platforms will need modification, but more importantly the Services must develop gateways and relevant infrastructure to share information in a ubiquitous and seamless fashion.

This has become “industry standard” for civil commerce, and it must become the new normal for the U.S. military. Platforms must become “cloud ready” in terms of communications and information management. Some platforms may require modifications, such as avionics bus structural improvements to permit greater data off boarding, and subscriptions to a variety of external data sources.

The concepts of Net-Centric Military Operations, the Joint Information Environment (JIE) and the Joint Airborne Layered Network (JALN) attempt to address the needs mentioned above by establishing performance parameters for the acquisition of IT systems.

These performance requirements apply to any system capable of creating information, such as platforms, weapons, and even handheld devices. This vision would direct DoD to take advantage of current and emerging technologies that would allow new systems to plug-and-play into a common information exchange.

Creating this plug-and-play operational network for DoD will be a multi-prong, multi-step process. DoD must establish a core operational information exchange to which new systems will connect.

For example, joining Link-16, the dominant tactical data link, to the DoD information network through multiple pathways such as ground terminals or a Joint Airborne Layered Network, would create a broad foundation to build such a network.

Another approach is to create gateway-based solutions, such as the Battlefield Airborne Communication Node, or BACN, to connect currently fielded disparate networks, waveforms, and platforms.

Yet another concept is to equip each platform with its own translator to accomplish the role of a few gateways thus contributing to the distributed and robust nature of a notional Combat Cloud.

To become a fully informationized force, all future capabilities will need the architecture and necessary protocols to connect through gateways with individual translators or to existing networks.

Ultimately, a plug-and-play concept may allow current disparate networks and systems to seamlessly share and access information.

This does not mean every Service has to buy the same equipment—nor does it impose the unobtainium of a common operating standard. Experience, physics, tactics, or the combat environment may dictate that some systems should be uniquely designed not to operate with others.

Nevertheless, normalizing data link frequencies, waveforms, and content format or requiring unique systems to provide a gateway gives a Joint Force Commander the flexibility to fully command battle networks and control globally distributed forces.

So how did we get here? Despite the explicit acknowledgment that future forces will need to operate and defend battle networks, progress toward building fully integrated battle networks has been sporadic and inconsistent, and without an overarching vision.

Currently, the DoD is bogged down with dozens of programs and concepts of operation, each being developed independently lacking a coherent effort that reconciles gaps or redundancies.

Since communication systems were primarily created to facilitate command and control and battlespace awareness, they have traditionally been viewed as supporting capabilities that simply enhance primary combat tasks. This has resulted in the piecemeal approach to fielding information systems and communication networks.

For example, the primary data link for aircraft of the U.S. and NATO is Link-16. One of the key data links used by U.S. Army and Marine ground forces, is the Enhanced Position Location Reporting System or EPLRS. EPLRS does not directly share information with aircraft that could perform close air support.

To rectify this communication problem, the U.S. military modified EPLRS radios and put them on aircraft and created the Situational Awareness Data Link (SADL). Now, SADL equipped aircraft could communicate with each other and EPLRS surface forces, but not Link-16 equipped aircraft!

Unfortunately, these types of challenges continue to exist. Currently, there is no data link between the F-22 and the F-35 that allow them to share targeting data. Instead, these two 5th generation aircraft operate separate networks riding on proprietary links.

Incredibly, the U.S. military continues to field many closed networks essentially creating private clouds that cannot share information. Other examples include isolated special operations networks; ISR platforms that use proprietary means to communicate with their ground nodes; and ship-to-ship networks that are crypto-isolated.

So how do we change this situation to best achieve information access and control? The capability already exists for current battle networks to translate collected information into a common format so other systems are able to access and process the information.

Future joint force operations will need an even greater ability to establish multiple network paths that function across a broad range of frequencies.

More importantly, future battle networks must provide combatant forces with a number of functions available using a cloud-type access. These cloud applications should include:

- Positioning, navigation and timing (PNT). GPS currently provides this capability but it is quickly becoming an irresistible cyber target.

- Collaborative communication. This includes services like text, chat, and voice and also asynchronous services like e-mail and file sharing.

- Track management and correlation. Building a Common Operating Picture requires algorithms that correlate entities in the battlespace; distinguish between multiple objects; resolve single objects; and maintain continual “custody” of basic information about those objects such as location and status.

- Combat identification. Beyond establishing an object’s location and status, it’s important to identify whether it’s friendly, hostile, or unknown. This is a significant deficiency in today’s complex battlespace, and would be a valuable service that could be provided through a cloud architecture.

- Intelligence updates. This may be as specific and detailed as individual target folders with updated intel products, or may be general information about an area of interest.

- Information Control. The ability to share information across multiple security domains, and classification levels, must be a central feature of any combat cloud. Various combat elements will be connected to networks with unique dissemination caveats, and the gateways and system protocols must honor those through automated rule sets.

- Fusion. A critical function of the combat cloud will be providing a way to fuse all of the information available. One application of fusion is to add greater fidelity to tracks that have already been correlated. This will require sophisticated algorithms and perhaps man-on-the-loop to reconcile disparate elements of data.

We must also assume that any operational environment will be contested. So solutions must be devised to achieve assured connectivity. I believe this will be one of the toughest nuts to crack in achieving the promise of the combat cloud, because potential adversaries recognize its potential, and are acting to prevent it.

Any information the system cannot share due to enemy counters could be stored for future routing as threat levels change. Some information may simply be lost because of heightened threats or a severely contested environment. So we must also learn to fight in these environments and not simply assume we will always be able to effectively defend against them.

Meeting these and other potential information requirements will require balancing the functions of sensing, processing, fusing, storing, communicating, and acting across the all the domains and elements that make up the combat cloud.

During combat operations, every system that detects external stimuli is a sensor. For example, the AIM-9X Sidewinder missiles with their IR staring focal planar array seekers, or a KC-46 refueler’s weather mapping radar both qualify as sensors.

Under DOD’s program-based organization, however, too often the narrow focus of program optimization results in missed opportunities to integrate, analyze, and interpret information of value to war fighters and decision makers. For example, most combat aircraft in the US military have some type of sensor on board, yet virtually all of that potential information is figuratively left on the floor of the cockpit.

In the current program-centric budgetary world of the DOD, narrowly focused optimization of individual platforms, sensors, and weapons is the norm. Absent a clear definitive vision, and without a strategy to realize that vision, the big picture is lost among a collection of dispirit, disconnected systems, that are often kluged-together to pass as joint.

This is why we need a vision...Future joint operations will require concepts and practices for how to join together and command and control desired effects; and distributed battle, intelligence, and surveillance networks.

Commanders must change the way they view networks and information systems. Rather than value only the weapons and platforms that launch them, commanders need to recognize the value of information and the effects they can create based on connectivity and optimal use of the electromagnetic spectrum.

This shift in perspective is necessary if the U.S. military is going to overcome the institutional structures that currently prefer platforms to spectrum. Prioritizing how U.S. forces could be networked together to collect, share, and protect information will reduce unnecessary redundancies and archaic equipment. Moreover, gaps in capabilities such as the lack of connectivity between 4th- and 5th- generation aircraft will become obvious deficiencies that require correction.

Becoming a fully informationized force will require leaders to recognize that information is a combat resource that must be controlled and protected by fielding weapon systems integral to creating a Combat Cloud.

If the Combat Cloud is developed properly, it promises to yield an expansive, redundant defense complex with radically enhanced data gathering, processing, and dissemination capabilities for all operations.

In an era of constrained resources for defense, and order of magnitude increases in warfighting capability such as directed energy weapons, perhaps the best bet on achieving a third offset strategy is the notion of actualizing the Combat Cloud.

The attributes of the Combat Cloud will offer tactical, operational, and strategic level actors dramatically enhanced situational awareness by transforming disparate data into decision-quality knowledge while expanding the range of options available.

This vision represents an evolution whereby individually networked platforms transform into a broader system of systems enterprise integrated through domain and mission agnostic information linkages.

This approach will not only change the way we define new requirements, but more importantly, the way we think; command, control; and operate those systems.

Central to the combat cloud vision is the control of information across the battlespace. By identifying ongoing vulnerabilities with cyber warfare; requirements to establish secure connectivity; and the necessity to analyze big data; this approach implicitly acknowledges that winning the next war will hinge not only on access to information, but protecting that information as well as exploiting it in attack operations.

Cyber Operations, Space Operations, and Electromagnetic Spectrum Operations can be simultaneously conducted against targets using different portions of the Electromagnetic Spectrum. All of these must be integrated as fundamental elements of the combat cloud.

Rear Admiral Peter Fanta, the current OPNAV Director Surface Warfare recently articulated a vision for the Navy of “if it floats, it fights” based on a concept of “distributed lethality.”

Likewise, the Mitchell Institute of Aerospace Studies’ symposia over the previous year and associated discourse on the subject of constructing the Combat Cloud reflects a vision of constructing an ISR / Strike/maneuver/sustainment complex where “every sensor is a shooter, and every shooter is a sensor.”

This is the essence of the Combat Cloud—it’s not just the network—it is the entire enterprise of sensors; shooters; and connectors all part of a cohesive, coherent whole and it must extend across all operating domains if it to realize its potential as the basis of the next offset strategy—if not the offset strategy itself.

Now, to fully capitalize on these capabilities will require a new way of designing our force. We have to think outside of the organizational constructs that history has etched into our collective psyche. Cloud-centric, interdependent, and functionally integrated operations are the keys to future military success.

The future needs an agile operational framework for the integrated employment of U.S. and allied military power. It means taking the next step in shifting away from a structure of segregated land, air or sea warfare to integrated operations.

The central idea is cross-domain synergy. The complementary vice merely additive employment of capabilities in different domains such that each

enhances the effectiveness; and compensates for the vulnerabilities; of the others.
A tremendous strategic advantage will accrue to the US and our allies if we exploit both technological as well as organizational innovations to develop this capability.
This combined effects approach is about integrating existing and future operations across all the domains with an agile operational framework guided by human understanding.
It’s an intellectual construct with technological infrastructure, and requires dominance of the electromagnetic spectrum at the appropriate times and places.

The 9/11 commission report's now famous summary that the cause of that disaster was a "failure of imagination" cannot be allowed to be repeated. It’s time to do a bit of imagining—imagining how we can restructure our legacy EW organizations and processes with the cyber domain, and integrating emerging directed energy capabilities, to best meet the conditions of the information age.

This will not be easy and it is sure to upset many apple carts, but if we don't do it, our adversaries will—and we have too much at risk to let that happen.

All you who are assembled here for this conference have the spirit, capability, drive, and intellect to make that happen. I encourage you to take advantage of this conflux of talent, and together you’ll create a set of capabilities that will actualize our Nation’s ability to succeed in any challenge.

Thanks for the privilege to share this afternoon with you. I wish you all the best as you create the way ahead to achieving the vision of a combat cloud.

-- END REMARKS --