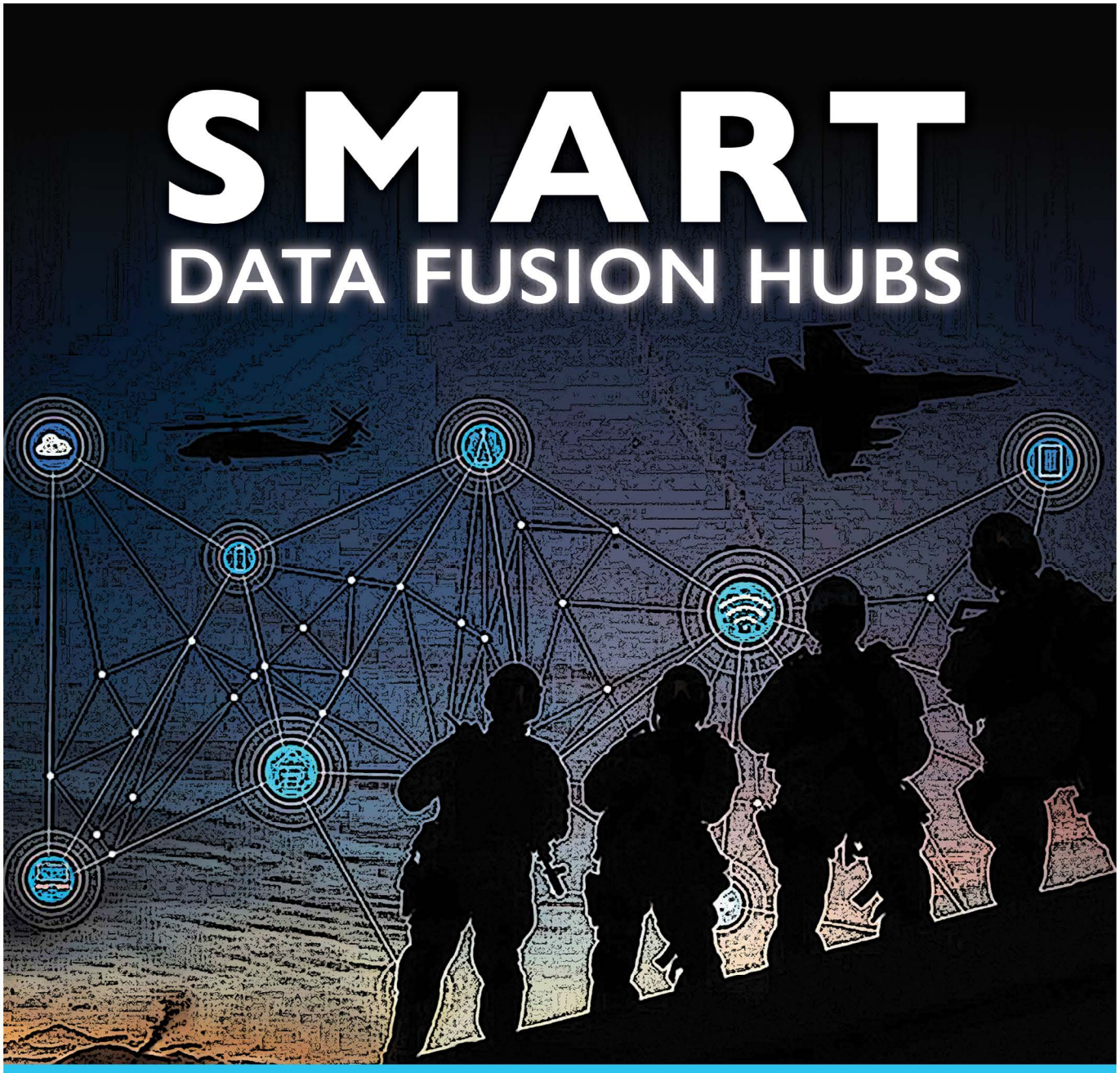
SMART
DATA FUSION HUBS



FOR MULTI-DOMAIN OPERATIONS

EXECUTIVE SUMMARY

Data fusion at the tactical edge is a top requirement for multi-domain operations.

US military forces are extremely reliant on fast, accurate flows of information at the tactical edge. By the 2010s, a range of grey, black and khaki "boxes" were creating fast, adaptive data nets all over the battlefield. Some were lightweight, low-power line-of-sight links between ground forces. Others connected air and ground forces over radio frequencies, sharing full-motion video, for example. Still others relayed sensor data from manned and unmanned aircraft, and space satellites.

The US-led Coalition was on the net all the time in the peak of anti-ISIS fight from 2014-2018. A reliable combat network became as central to daily operations as a smartphone to civilians.

But Russia, China and others were watching. In future fights, adversaries will use electronic warfare jamming and cyber operation to break up US combat networks. Russian electronic warfare in Ukraine and Syria, plus China's activity in the South China Seas demonstrated the threats to current battle networks. "They've gone to school on us," noted one US Army general.

The next set of battle networks must go well beyond the data sharing connections achieved in battles in Afghanistan, Iraq and Syria.

The double shock of network dependence plus adversary threats pushed the Army, Navy, Marine Corps and Air Force toward multi-domain operations. Multi-domain operations elevated space, cyber and electronic warfare and acknowledged that commanders must link sensors and forces across all domains.

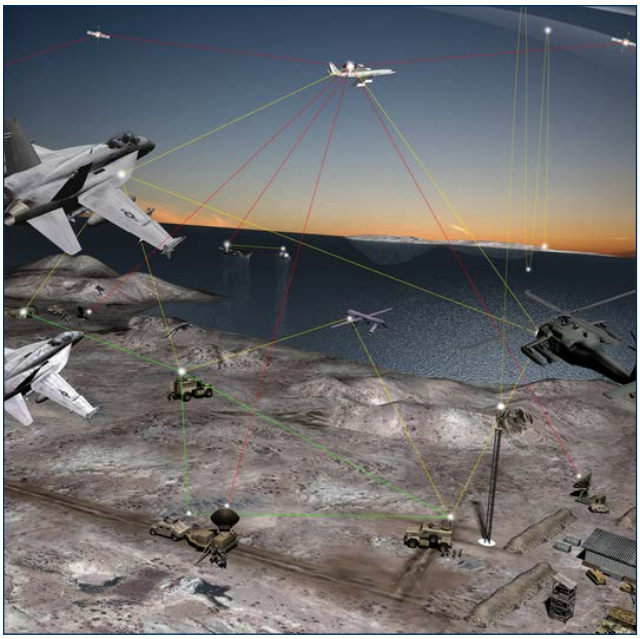
Multi-domain operations will generate an exceptionally high demand for distributed processing, data fusion and autonomy.

The technology is ready to introduce smart data fusion hubs: a new type of data link with secure waveforms and greater functionality. In experiments over the past five years, American industry has demonstrated success with open systems architectures, encrypted links, secure waveforms and smart data processing. These are the essential ingredients for a leap ahead in battle networks.

The "boxes" in development today are the jumping-off point for the next set of data fusion capabilities. Instead of pumping more and more data, what's needed are smart data fusion hubs to process, sort and refine data, in real time, while operations are underway. Smart data fusion hubs can create efficient, secure processing at the forward tactical edge. Over time, the connections and processing power of smart data fusion hubs also open the door to insert complex artificial intelligence capabilities into battle networks.

Preliminary testing of networks with smart data fusion hubs could begin before 2020, given sustained effort. Many promising technologies will be ready for battlefield experimentation within 12-36 months. The challenge is to pick out promising candidates, set up cooperation between the Services and speed up experimentation for delivering multi-domain solutions to the joint force.

One of the major reasons for moving fast to experiment with smart data fusion hubs is to strive toward an enterprise solution. The Department of Defense's task is to modify existing and near-future DoD platforms to take advantage of the full potential for data fusion. By all rights, US forces should be far, far ahead in their data access and utilization. Multi-domain operations count on it.



SMART DATA FUSION HUBS

FOR MULTI-DOMAIN OPERATIONS

Table of Contents

By Rebecca Grant

Cover and Layout by Dixon Designs.
Printed in the United States of America.

INTRODUCTION

The US military is undergoing a fundamental shift in how it operates. The highly-networked force required for precision operations is at risk, unless the Pentagon accelerates advanced technology for secure communications, data fusion and tactical networking.

"It's a unique period of time in the US military. The joint chiefs, we've all fought together," said Air Force Chief of Staff General David Goldfein. "And you will hear us all talking about this concept of multi-domain operations."

Over the past 15 years, US forces have become dependent on the unchallenged flow of data across combat networks. Credit the huge growth of airborne ISR and many types of links between deployed forces after 2001. US forces in Afghanistan and Iraq learned to link soldiers on the ground with aircraft and other sensors to see and strike the enemy. Command centers added in other intelligence information and patterns of life to learn how the enemy moved and where to intercept and destroy. Forces came to rely on improvised aerial networks for everything from relaying communications in the mountains of Afghanistan, to distributing powerful F-22 sensor data to other combat aircraft striking Syria in 2018.

An innovative batch of communications links came out of those wars – and they added more computer processing and software-defined features. By the 2010s, a range of grey, black and khaki "boxes" were creating fast, adaptive data nets all over the battlefield. Some were lightweight, low-power line-of-sight links between ground forces. Others connected air and ground forces over radio frequencies, sharing full-motion video, for example. Still others relayed sensor data from manned and unmanned aircraft.

The networks were never perfect, but they enabled cross-domain operations.

However, the Russians were watching. Russia, China and others can now contest US information dominance, and undermine multi-domain operations. In the Ukraine, Russian forces used a variety of electronic warfare techniques to zero in on targets with lethal results. China also stepped up its electronic warfare, cyber and space capabilities.

Solutions for multi-domain operations require more data capacity and security. But a crucial piece is missing: data fusion. No one is setting up the data hubs to form the intelligent, networked system that can share the right information across the joint force and mature it into enhanced decision support for rapid action. Yet these rapid decisions will be the margin of victory in peer conflict. Data fusion in combat networks is essential to achieve multi-domain superiority.

The Services have never worked together on communications. Now they must.

Many promising technologies will soon be ready to test out. Top of the list is a new type of box: a smart, data fusion hub that forms the network and swaps data at much higher rates. With enhanced processing power, smart hubs can sort and prioritize data, and pioneer automated decision support techniques. Choices are many, but time is short. It's time for Congress and the Pentagon to stimulate experimentation with smart data hubs to make the next generation of wireless networks secure and effective for true multi-domain operations.

BACKGROUND: BATTLE NETWORKS

US military forces are extremely reliant on fast, accurate flows of information at the tactical edge. Powerful aerial and space networks link forces on the ground with manned aircraft, unmanned aircraft, tactical operations centers, command posts and a wealth of intelligence data.

A generation ago, airmen flying missions in Operation Desert Storm communicated mainly with voice over radio. A few big computers generated plan-

ning orders at air operations centers but they weren't linked to other computers.

Tactical edge networks emerged in Afghanistan and Iraq in the 2000s. Internet protocols opened the door for secure chat, useful for planning and controlling missions. Early on, these networks were small clusters that expanded on existing secure data links like Link 16, which joined air battle platforms on big aircraft like AWACS to fighters like F-15s and F-16s. Data flow was limited but secure.

Hunting for terrorist targets demanded more real-time ISR products – especially imagery and full-motion video – be passed to multiple aircraft and to controllers on the ground.

American industry responded with a hasty collection of portable radios and datalink boxes. One of the first innovations was L3 Tech's ROVER. It started as a link installed on the AC-130 gunship to receive Predator drone video. By 2005, after significant investment by L3 Tech accelerated development, ROVER was reconfigured as a software-definable radio and smaller devices fitting into backpacks. Airmen on the ground could share a video link to pilots in cockpits. "I can circle an area on my screen, drawing arrows for emphasis, and what I'm drawing appears on the pilots' screens as well," said SSgt. Justin Cry, a JTAC from Shaw AFB, S.C. "The pilots can look exactly where we need them to look." [i]

As more forces deployed to Iraq and Afghanistan, secure networks between aircraft and ground controllers became essential to operations. Joint forces began to rely on their effects.

Enter the boxes. ROVER was, in its new form, a "box." It had been miniaturized and upgraded, still functioning as a portable radio receiving sensor data from many platforms, and able to transmit that data along the tactical network.

In 2007, near Baghdad, human intelligence tipped off planners that a roadway was mined with improvised explosive devices. TSgt. Mike Cmelik, an Air Force JTAC, used a ROVER to communicate with a B-1 bomber which released seven tons of bombs during three passes on the target. Air operations centers piped in surveillance from U-2s, Global Hawks and space satellites.

"The airborne component of ROVER is a video link module – a black, metal box a little smaller than a shoebox – that fits neatly into an existing space in the LITENING-AT targeting pod. It transmits through a small, round antenna that sticks out about an inch from the bottom of the pod and has the diameter of a silver dollar," explained the Air Force in 2010.

ROVER and other devices soon filled the battlespace with improvised, aggregated networks based on transceiver boxes looping in aircraft, command centers and ground forces. These emerging tactical networks relied on software-defined radios capable of supporting wideband waveforms. The waveforms carried voice, internet messaging, and imagery, all with encryption.

When more range and capacity was needed, the improvised aerial networks expanded to include aerial gateways like the Battlefield Airborne Commu-

nications Node. The BACN node flown on aircraft like the RQ-4 Global Hawk and E-11 acted as a relay and translator linking up different radios in the battlespace. The BACN payload "can extend the range of a radio signal or bridge it to another radio, it can combine data links, and it can take one type of communication device and connect it to another type of communication device, like a telephone to a radio," said Lt. Col. James Peterson, commander of the 430th Expeditionary Electronic Combat Squadron based at Kandahar.[ii]

Other technology improved data exchange. For example, the Tactical Targeting Network Technology (TTNT) developed an Internet-protocol format to share sensor data, voice and video transmission at ranges up to 300 miles. TTNT was designed to accommodate up to 200 users who could join or exit the network as needed. TTNT featured in a series of joint operational exercises beginning in 2004, as well as at the USAF's Red Flag and other exercises. The Navy experimented with TTNT in 2017, but observers noted full implementation of TTNT would require "vast amounts of new hardware" and still be susceptible to future jamming.[iii]

Teaming so many assets together produced remarkable effects – especially when there was a well-positioned gateway like the U-2 reconnaissance plane. "I was listening to a convoy force," said U-2 pilot Lt. Col. Matthew Smith of a mission over Afghanistan in 2012. The convoy had stopped for vehicle problems when U-2 imagery revealed Taliban forces heading to ambush them. "They don't know there's bad guys around the corner," Smith realized. He radioed the convoy to lock down and contacted two Navy F/A-18s on an overwatch mission nearby. "You could hear the gunfire" Smith said as the Taliban attacked. Within minutes the F/A-18s dropped weapons breaking up the firefight.

Teaming multiple streams of intelligence to generate predictive analysis was the logical next step. Network Centric Collaborative Targeting or NCCT was set up as a formal Air Force program to look ahead to standards and architecture for data fusion. It twined ISR data from different streams of intelligence – merging the beeps and squeaks of signals intelligence with the glowing radar dots of ground moving target indicators, for example. NCCT ingests data from ISR platforms and links to ground stations to produce a single, composite track showing the location and identification of a high-value target. That might be an enemy air defense threat emitter, or a terrorist vehicle convoy.

The US-led Coalition was on the net all the time in the peak of anti-ISIS fight from 2014-2018. Through the tactical networks came full motion video, real-time reconnaissance, improvised communications links and fire support for troops in contact. A reliable combat network became as central to daily operations as a smartphone to civilians.

But there were two problems. Effective as they were, the networks had obvious gaps and shortfalls from the start. Range of transmission and data rates were limited. Combat aircraft in theater might have dissimilar radios for their tactical data links. Often communication paths were "lost, denied or unavailable" as an Air Force study put it.[iv]

Just as critical, the surge in tactical communications from 2001 to 2014 took place in a benign environment where the enemy rarely interfered. With all sides trying to use more data, the counter, of course was to break up the opponent's data flow.

And Russia was watching.

RUSSIA, CHINA AND OTHER THREATS

"They've gone to school on us."
– Lt. Gen. Bruce T. Crawford,
U.S. Army Chief Information Officer

Call it lethal static. In future fights, adversaries will use electronic warfare jamming and cyber operations to break up US combat networks.

Adversaries in Syria and elsewhere are testing the US every day. And it's clear that Russia, China or adversaries with their caliber of equipment will send up tornadoes of electromagnetic interference and hack any communications links they can touch.

Rival militaries have studied US technology and tactics. US dominance of battle networks is under threat. Wily adversaries continue to develop capabilities designed to deprive US forces of their battle networks by attacking data sources and connections.

"They've ended up with killer capabilities, jamming in a multitude of frequencies for hundreds of kilometers," said one analyst, adding that the Russians "know all of our vulnerabilities." [v]

Russian operations in Ukraine were a tipping point. In 2014, Russia helped separatist forces in Ukraine use advanced counter-battery radar and UAVs to accurately pinpoint Ukrainian government forces, specifically their command and control. "Ukrainian commanders are telling us that within minutes of coming up on the radio, they were targeted by precise artillery strikes," said retired Marine and former Deputy Secretary of Defense Robert O. Work in a 2015 address to the Army War College. [vi]

Russia also penetrated and disrupted tactical networks, and the flow of information to soldiers. "This capability deployed against Ukrainian govern-

ment forces and enabling access to soldiers' means of communications aims to undermine and degrade troops' morale," wrote one analyst. [vii]

Imagine being under intensive, precise Russian artillery fire and having your smartphone, military radio and command post communications go dead.

"Because of maneuver warfare's reliance on communication, Russia has invested heavily in electronic warfare systems which are capable of shutting down communications and signals across a broad spectrum," warned the U.S. Army's Asymmetric Warfare Group in December 2016. "The Russians layer these systems to shut down FM, SATCOM [satellite communication], cellular, GPS, and other signals." [viii]

Russia equipped several electronic warfare units with systems including:

- Tracked ground vehicles like the Murmansk system, with 32-foot high antennae reaching up to 5,000 km in the HF band
- Jammers for X and Ku-band frequencies often used by US fighter aircraft
- GPS jamming on mobile cellular phone towers
- Fake SMS messaging to phones on 3G and 4G networks

"If you take a look at what's going on in Ukraine and other places, they are fracturing our way of war by using other domains," said Army Gen. David G. Perkins. "We've seen them be able to take down large land forces with a combination of electronic warfare, cyber, autonomous systems, drones, et cetera – not with a close-in battle." [xi]

"The Russians have continued to move forward with their EW modernization. They have demonstrated the ability to completely shut down everything the Ukrainians are using in terms of communications," said Army Lieutenant General Ben Hodges during his tour as Commander, US Army in Europe.[x]

Russia also transported much of this equipment to Syria for further battlefield experimentation. Syria today presents the "most aggressive [electronic warfare] environment on the planet from our adversaries," the head of Special Operations Command Gen. Raymond "Tony" Thomas said in 2018.

"If our tactical command posts can be found, then they can be killed," said Lt. Gen. Bruce T. Crawford, who was Army Chief Information officer. He went on to say "if you examine closely the electro-magnetic signatures of our command posts, they are not survivable." [xi]

Then there is the Pacific. China shifted its strategy towards "information wars" over a decade ago. China's military strategy opposes what they term "close-in air and sea reconnaissance and surveillance against China" and calls for an integrated combat force to "prevail in system-vs.-system operations featuring information dominance, precision strikes and joint operations."

In 2018, it came as no surprise when China installed electronic warfare jamming equipment on its fortified bases at Fiery Cross Reef and Mischief Reef. In July 2018, China's military ran a major electronic warfare exercise with 2100 participants at five separate bases. China's buildup in the South China Sea "just expands on the potential for electronic jamming," said RADM Nancy Norton, the deputy director of Navy cybersecurity. [xii]

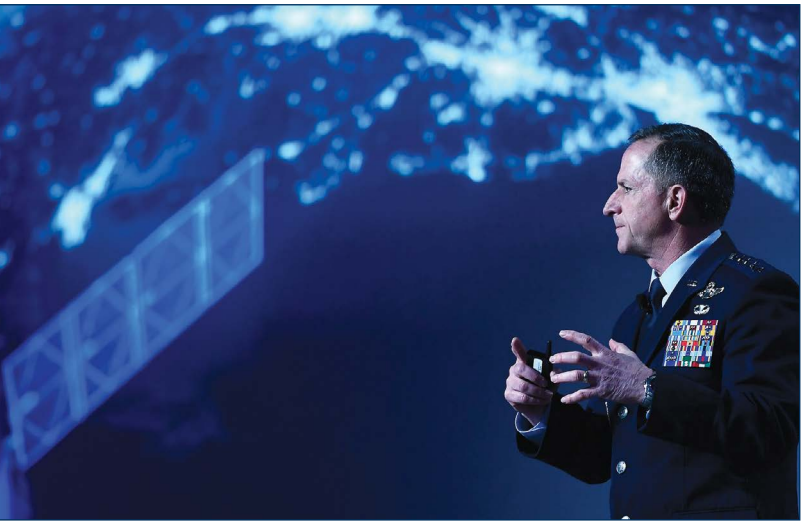
"Potential EW victims include adversary systems operating in radio, radar, microwave, infrared, and optical frequency ranges, as well as adversarial computer and information systems," warned the Pentagon's 2018 China report. China upgraded wingtip electronic warfare pods on their J-15 navy fighter and on several UAVs.

China is also working toward "emerging technologies such as big data, internet of things, and cloud computing to provide reliable, automated platforms that further increase process efficiencies." China is embracing "big-data analytics that fuse together a variety of data to improve automation, to create a comprehensive, real-time picture. Passive capabilities – like covert cyber intrusion – may present another scary threat to the tactical data flow, too.

"We are moderately prepared for the low-end fight like we've seen in Iraq and Afghanistan. That's what we've been doing," Rep. Don Bacon said. "But in a high-end fight, we are not prepared." [xiii]

Not "the planes or ships or what have you – it's the computers we need to connect." That was USAF Chief of Staff Gen. Goldfein's succinct summary of multi-domain operations.

The double shock of network dependence plus adversary threats helped push the Army, Navy, Marine Corps and Air Force toward multi-domain operations. The **Army** admitted in 2017 it was not "trained, equipped, organized or postured" for war with peers like Russia or China. The answer was cross-domain synergy and preparing forces "to fight across the breadth and depth of enemy capabilities, seamlessly reaching from battlefield to home station and across multiple domains." [xiv]



The **Navy** planned for a networked fleet. "So this is the realm of artificial intelligence, learning algorithms, figuring out the optimum way to team together the people, our sailors and machine assistance, to be able to sort through that amount of data, and get to those decision-relevant bits of information as quickly as possible," said Chief of Naval Operations Admiral John Richardson. "Competing in that orient and decide part of the OODA loop, so that we can beat the competition in that part of that loop," Richardson added.[xv]

The **Marine Corps** Commandant General Robert B. Neller laid out a new approach to multi-domain amphibious operations emphasizing maneuver and information. "It's going to be a land, air, sea operation, but it's going to involve space, it's going to involve information, it's going to involve the electromagnetic spectrum; all things that we haven't had to think about in the past 15 to 20 years," said Neller. [xvi]

The Air Force quickly recognized that "multi-domain warfare also means response in any dimension. An attack on space capabilities can be met with cyber in the electromagnetic spectrum domain or a response from any other domain or combination of domains."

To this end, the **Air Force** budgeted for multi-domain command and control starting in 2019. "Integrating capabilities that span all domains of warfare will be required for success in future combat. We are advancing our command-and-control systems to reflect the changing character of warfare. This approach will network sensors from space, air, land and sea, and fuse information to create a more comprehensive picture to support the joint fight, even in a highly contested environment." [xvii]

Multi-domain battle recognizes that domains have expanded and that it will always take a melding of several domains to achieve superiority. Here's how Admiral Harry Harris, General Robert B. Brown, Admiral Scott Swift, and Dr. Richard Berry painted the picture for multi-domain operations in the near term:

> Imagine an F-35 acquires a target at sea – an enemy ship – and then passes the track data through a command and control system (e.g. Link 16) to any potential military unit with appropriate munitions and within range of the enemy ship. This information is passed through a gateway to the Joint Range Extension Applications Protocol enabling the transmission of tactical data messages long distances via the Internet using the Battlefield Airborne Communications Node in a U.S. Air Force Global Hawk. This tracking data can then be passed to military units on land, air, or sea such as the Paladin artillery system or the High-Mobility Artillery Rocket System (HIMARS). The Paladin or HIMARS then kills that enemy ship from the land.

To summarize, this is a Navy fighter communicating through an Air Force unmanned aerial vehicle with an Army or Marine ground-based weapon system

to kill a sea-based target – and for the most part this can be done today, with small improvements to the technological communication links between the services. [xviii]

The scenario sketched above showed that the next set of battle networks must go well beyond the data sharing connections achieved in battles in Afghanistan, Iraq and Syria. Multi-domain operations – or whatever they will be called in the future – will generate an exceptionally high demand for true data fusion. It's not just secure connections. Achieving superiority in multi-domain operations will depend on networks that can provide a higher degree of distributed processing, data fusion and autonomy.

Think of data fusion as melding different types of data (images, video, emitter signals) from different sources, then transmitting just the most needed elements to the right users, all in real time.

Conflict in the Pacific, for example, demands space-based transmission of tactical data. To give multi-domain operations global reach and reaction capability, space assets are vital. The technical challenge ahead is to introduce "boxes" with communications fusion and cognitive power – and build them as enterprise solutions reaching across Service platforms. "Connecting the computers" requires a deliberate leap forward to battle networks that can autonomously relay, process and share smart data.

If the US can develop smart data fusion for joint service battle networks, multi-domain operations can become a reality.

MULTI-DOMAIN OPERATIONS HAVE FOUR MAIN ELEMENTS

❶ **First**, air, land, sea, etc. must be linked so that commanders can use forces from all domains to track and fire upon a hostile target. A space sensor may see a missile launch, pass the information to an aircraft, then to a ship, which directs fires from a land-based anti-missile system.

❷ **Second**, multi-domain operations elevate the space, cyber, and electronic warfare information domains to equal status with other physical domains.

❸ **Third**, multi-domain operations depend on continuous, efficient information flow for many functions, including surveillance, fires coordination, logistics, management of manned-unmanned teaming, etc.

❹ This leads to the **fourth** characteristic: US forces must have assured, protected information dominance in the fight – and reach for data fusion at the forward edge.

While multi-domain battle concentrates on combat, logistics and combat support functions also depend on domain dominance.

BETTER BOXES AND BEYOND

"I don't want to do processing, exploitation and dissemination in a reach-back mode in the future. I want to process, to exploit right on the aircraft or right on the sensor so that I can actually take that data, condition it, and then use it with other data."
– Lt. Gen. VeraLinn Jamieson, USAF, Deputy Chief of Staff for ISR

Data fusion at the tactical edge is the next step required for multi-domain operations. Instead of pumping more and more data, what's needed are the "boxes" to process, sort and refine the data, in real time, while operations are underway.

The "**boxes.**" As discussed, tactical data links today depend on a bunch of boxes: digital units that transmit, receive and direct data around the battlespace. Some, like ROVER, were small enough to carry by hand. Others fit onto the smaller unmanned planes. Still others are installed on larger systems like Global Hawk and on manned aircraft. For example, L3's Bandit was designed as a lightweight, low-power link running at up to 6 mbps. The larger Compact Multi-Band Data link allows 45 mbps transmission in Ku, C, L or S-band radio frequencies – the heart of the military operations spectrum. Go up a level and there are transceivers for full-motion video and other types of situation awareness imagery.

What all the boxes do is utilize radio frequencies to provide communications gateways to link platforms and allow their users to enter the net-centric battlespace. When placed in an airplane or a ground control center the "box" functions like a superb router, accepting and directing information. Still, data like full-motion video is downloaded to review later.

But in Multi-domain Operations the new requirement is for data fusion at the forward edge. "Today, we take the data off," explained Jamieson. "In the next two to four years it will be processed at the sensor."

That means a new generation of "boxes" that can carry out data processing and fusion at the point of the sensor.

Data Fusion Technology. Over the past five years, several experiments advanced the technology for data fusion "boxes" and advanced waveform technologies. In 2013, an F-22 flying from Nellis AFB, Nevada, communicated with software on the F-35 avionics test aircraft, known as the Catbird. "We successfully integrated an F-22 with a tactical radio for Link 16 transmit and receive capability, and two L-3 Communications devices to support encrypted and secure operations," said Ron Bessire, who was then Vice President of Program and Technology Integration at Lockheed Martin Skunkworks. The test was dubbed Project Missouri after Air Combat Command leadership challenged the industry team to "show me" the capability. Hardware and software development took a speedy seven months. It was a sign of technical possibilities using open systems architecture, but also a marker of how hard innovators had to push to test out capabilities.

In 2015, the Air Force began work on a Common Mission Control Center at Beale AFB to enable "different unmanned aerial systems and manned platforms to communicate and operate as a coordinated family of systems in support of intelligence, surveillance and reconnaissance missions." This was a series of ground and air links creating global input to tactical networks.

BETTER BOXES AND BEYOND

In 2017, high-altitude platforms including the U-2 and Global Hawk flew with communications "boxes" containing systems for talking across multiple channels and processing data. A U-2 flew a developmental "Einstein box" enterprise mission computer during Northern Edge wargames in Alaska in 2017. The Einstein box was developed by Lockheed Martin "to let older-generation aircraft communicate securely with stealthy platforms like F-22s and F-35s," one observer explained.

The boxes in development today are the jumping-off point for the next set of data fusion capabilities. They incorporate new types of secure waveforms and greatly increase the processing capacity and data fusion functions in the tactical network.

Several protected tactical waveforms have also been tested. One test in 2014 paired an L3 Tech waveform with Intelsat to measure "modem and PTW performance against various interference and jamming tactics and waveforms."

The Chameleon waveform is a further advance in waveform security and functionality. Chameleon operates in a wide range, making it resistant to jamming. But Chameleon also works as a cognitive software engine that can sense the environment and make intelligent decisions in real time about how to manage the radio and network.

The Smart Data Fusion Hub. Technologies like these and others can soon lead to "boxes" that perform several combat networking and processing functions. They're best described as smart data fusion hubs.

A smart data fusion hub is an advanced type of software-defined radio transceiver "box" whose first job is to rope together currently-installed datalinks, such as Link 16, MADL and others. Ships, aircraft, etc. carry nodes to participate with the hub. The hub "box" configures data flow by priority – making it a "smart" hub. It also has an open systems architecture – meaning the smart data fusion hub should plug and play with many other types of systems.

Since this is a military system, it also has to be extremely secure. The smart data fusion hub uses a secure waveform that guards its secrets by changing shape so well that it eludes interception, as previously discussed. Advanced waveforms also increase capacity and functionality of the smart data hub.

But the smart data hub does more than connect. It also processes. Tactical edge processing takes the place of sending data back to command centers to interpret and sort. Processing at the forward edge is much more efficient and can actually reduce bandwidth needed (which as a side benefit again increases security.) Now the smart hub can also carry out data fusion at the sensor, within the network and in links to offboard sources.

In the aerial network, for example, smart data fusion hubs shoulder several tasks:

- Connecting users ranging from pilots in the cockpit to controllers in the field and at operations centers.
- Protecting data with secure waveforms that work on many frequencies to diminish interference from adversaries
- Adjusting the data flow according to the mission
- Reforming and rerouting network data flow to establish data flow priorities
- Expanding access to unmanned vehicles – alone or in swarms – to create manned-unmanned teaming in the combat network

Smart hubs can also serve as automated housekeepers of the networks: monitoring, restoring, repairing, proposing alternatives and reporting on network status. Hubs determine when to turn down the signal, how to prioritize data and where to find alternate paths for data under wartime conditions. As the USAF's multi-domain communications study pointed out, future networks need C2 nodes that can maintain connections even when under attack.

Smart Data Fusion Hubs in the Battle Network. Smart data fusion hubs put the processing power into the network. They can also accept off-board data from ground stations, archives, larger platforms, space assets, etc. Decision support tools start with basic categorization, and could move on to include autonomous processes directed by human military personnel. Data fusion occurs as data within the aerial network meets up with refined data products processed on or imported from outside the net through the smart hub.

For example, information on a hostile surface-to-air missile battery may reside in a data set drawing on open source information from social media, intelligence community products like space surveillance, and machine learning such as historical processing of behavior by similar units. The C2 node can push that information forward to combine with fresh tactical information, such as electronic emissions by the battery radar or infrared spotting in pilot reports.

Part of the task will be implementing multiple levels of security. Some types of information can move with minimal security. Other information will be highly protected. Smart hubs can assist with sorting that data, thus freeing up capacity on the networks. The smart data hubs must be able to handle data in any format, with any classification level.

Smart data fusion hubs will help provide decision support. This takes many forms, starting with the ability for warfighters to call up the slice of data they need to execute the next tactical step. Decision support at its best feeds rapid, selected information to allow US forces to act more quickly than the adversary.

Over time, the connections and processing power permit smart data fusion hubs to add more complex artificial intelligence capabilities. For example, the smart data fusion hub can be assigned to sense adversary EW or cyber threats and implement countermeasures to keep the networks running. The countermeasures may come from a library of predetermined options. Another example is use of neural networks for pattern recognition or to detect enemy military forces using the images, radio signals, cyber tracks, and so on.

A future tactical network may have several of these smart data fusion hubs flying on aircraft and at ground or sea surface sites. With several smart data hubs installed across the battlespace, they will be able to pick up many of the command and control functions now performed by large air operations centers, ground force tactical operations centers, etc. Together the smart data fusion hubs achieve the desired structure of a resilient, large-scale network.

Smart data fusion hubs are also the on-ramp for artificial intelligence functions. Future concepts across the services are counting on artificial intelligence to do everything from guiding self-driving truck convoys to determining courses of action for autonomous weapons.

But strong advances in AI won't come to fruition without the communications network to control them. Smart data fusion hubs offer a way to start building the architecture for AI.

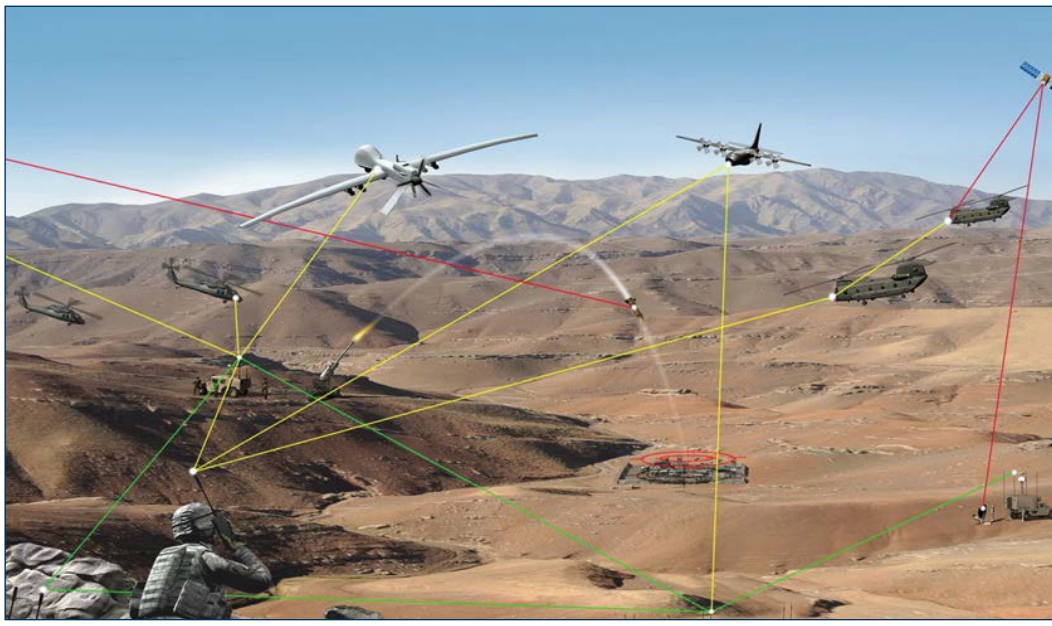
Forward battle networks need smart data fusion hubs to give the networks far more functionality. They must be able to support aircraft, ships, and unmanned platforms operating in lethal static and enemy cyber disruptions. Instead of throwing data back to massive processing at ground stations, these smart data fusion hubs can stand up networks that carry out the selection and processing of signals in the tactical network itself. This forward-edge fusion will sharpen attack options.

Smart data fusion hubs are also necessary for manned and unmanned systems to fight together. The Pentagon stood up a Joint Artificial Intelligence Center in June 2018. This was just the latest signal that military forces will be adding autonomy, manned-unmanned systems, machine learning and artificial intelligence products to future battles.

The best-known driver for automation is the glut of video. Video capture became integral to the US way of war during operations in Iraq and Afghanistan. Research is heading toward creation of a recurrent neural net, with artificial intelligence assets trained by humans to distill changes occurring in the battlespace. As this research proceeds, it will soon require a portal into the secure combat networks. Here again, a smart data hub will be needed to regulate the amount of information and timing of its entry into the combat net.

Smart data fusion hubs are also a good way to capture and control the benefits of autonomous systems, while maintaining appropriate levels of human control. A network capable of handling data fusion can regulate the balance of data and control for manned and unmanned operations. For example, the Army's strategy envisions smaller numbers of manned vehicles leading unmanned vehicles in resupply operations, for example. Those teams will rely on their connections even more, since many vehicles will not have a human crew back-up on board. Teams of manned and unmanned vehicles will depend heavily on access to smart data hubs.

Here again, the requirement for smart data hubs is urgent. Rivals are racing to infuse artificial intelligence into their militaries. Russia's goal is to replace 30% of military technology with robotic and automated systems by 2025. China wants robotics and AI to position China's military to dominate "intelligentized" warfare.[xxii] China "is approaching the use of AI just like the US approached going to the moon in the sixties," said Larry Lewis of the Center for Naval Analyses.[xxiii]



A TWO-YEAR PLAN

"If we do it right, then multi-domain operations will be so powerful that nobody will be foolish enough to mess with us because they know they would lose. To me, that's the ultimate success." [xxiv]

– *Gen Robert Brown, USARPAC*

Smart data fusion hubs for multi-domain command and control may be one of the most exciting and crucial Pentagon efforts since the precision targeting revolution of the 1990s. It affects all aspects of USAF operations and remains at the core of Army modernization. Navy integrated fires will rely on it too. Make no mistake – it's also a supreme test of space integration.

But it's undeniably a management headache. The Services are still set up to field major programs – satellites, ships, helicopters, etc. Both the Services and the Pentagon scatter communications and networking across multiple requirements and acquisition offices. The wartime rush to purchase the "boxes" and other components for the early networks didn't help. Procuring smart data hubs – in fact, just writing requirements for them – will be difficult, despite the maturity of the technology as provided by American aerospace industries.

Success requires looking beyond platforms. Military leaders must confront new issues with unmanned systems, autonomy, and machine learning to get the most out of multi-domain operations. The need for smart data hubs resides in the "white space" of new thinking.

That's why experimentation is so critical. It's not just about testing technologies – warfighters need hands-on experience to develop the tactics that come with data fusion. The best approach may be to experiment vigorously with secure networks enabled by data fusion hubs. Experiments can help fill in answers on how much data fusion throughput is needed, what type of nodes to install on platforms, and so on.

Past experience proved the value of experimentation for refining network requirements. BACN was developed via official joint experimentation exercises (JEFXs) in 2006 and 2008. The Predator drone fired a Hellfire missile for the first time after a 61-day

program in 2001. ROVER, as discussed, advanced quickly by going through many battlefield iterations before it became a program of record. Advanced technology concept demonstrations helped forge the Navy's Cooperative Engagement Capability and the Air Force's net-centric targeting. These developed in the early 2000s when battle networks were embryonic.

Unfortunately, tight budgets drove experimentation out of favor. The US Joint Forces Command (once commanded by General James Mattis, USMC) closed down in 2011.

Experimentation is now a responsibility that rests with individual services. "Under Joint Staff policy for concept development, experimentation begins after concept development. This may be adequate for narrow concepts or mission/domain capabilities where one Service has the lead. But this approach seems ill-suited for complex and multifaceted warfighting concepts such as MDB," explained two authors. [xxv]

What if the Air Force, Army and other services opted to move quickly to increase data fusion for multi-domain operations? Preliminary testing of networks with smart data fusion hubs could begin before 2020, given sustained effort.

- **Single platform integration.** Step one is for manufacturers to try a smart data fusion hub on a single platform, like a KC-135, JSTARS, P-8, or similar. Simulation may have to be followed by flying the data fusion hub on a test aircraft or a dedicated avionics test bed (like the ones aerospace companies use to test-fly mission software for major aircraft programs.)
- **Wartime priority.** Next, smart data fusion hubs should be installed across selected USAF and USN airborne C2 platforms. Deploying smart data fusion hubs in the Pacific and the Persian Gulf will provide real-world feedback on the effectiveness of adding more autonomous processing to battle edge networking. Initial tests merit a "wartime priority" to get the first increments of autonomy into the hands of service members.
- **Battlefield experimentation.** As technologies emerge, the Services should focus on rapid experimentation so warfighters can shape multi-domain command and control. With the open architecture construct, tactics, techniques and procedures can be developed in parallel while introducing emerging technologies. Congress can help with specific funding for experiments with smart data fusion hubs, on a tight timeline.
- **Strategy and Metrics.** As the USAF found with its AFWIC warfighting integration capability, tracking investment by platform is no longer sufficient to implement multi-domain communications upgrades. A systems approach is required. The Department of Defense should develop a specific, single strategy for adding smart data fusion hubs and other autonomous decision support to battle networks. The strategy should include short-term metrics to track concept development, funding and experimentation. Specific results from smart hub experiments can plug into Service concept and doctrine development.
- **Reports to Congress.** Congress could also ask the Department of Defense to report to specific Committees on multi-domain C2 progress, including smart hub experimentation. Remember, scaling up data fusion hubs is the type of program that will take constant shepherding.

Beyond this, experiments will quickly reveal the state of machine-learning algorithms as tools for multi-domain operations. The Pentagon's work on artificial intelligence processing of ISR data began in earnest only recently. Big questions lie ahead. One of the biggest is finding out where human operators are most important. For example, it's clear that humans must lead in developing the training databases whose millions of interactions educate the machine algorithms so they can identify objects on their own, for instance. A high degree of automation in secure network structure is essential to fend off interference and interception. However, the data fusion will still function best under what the military calls "mission-type" orders. Experimentation in the field is perhaps the fastest alternative given the revolutionary technologies at hand.

CONCLUSION

"Folks refuse to say the electromagnetic spectrum is a domain to dominate and have superiority in. I think that's a problem."
– Rep. Don Bacon

One of the major reasons for moving fast to experiment with smart data fusion hubs is to strive toward an enterprise solution – not letting the Services come up with multiple, overlapping or incompatible solutions for data fusion.

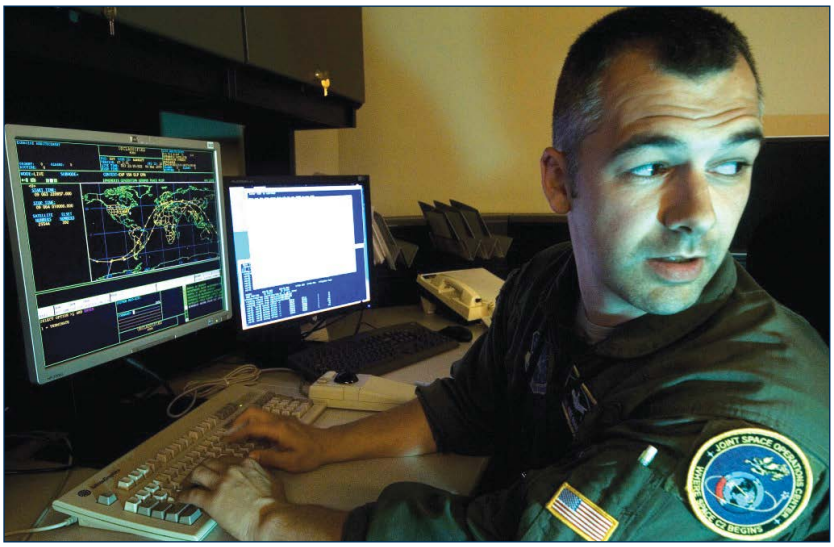
Research outside DoD has already delivered remarkable data fusion products. *Weather. Genomes. Social media analytics*. Many outside the Pentagon have already tackled information analytics. The emergence of cloud computing over a decade ago opened the door to software and hardware solutions to activate massive processing of data. Hadoop processed a terabyte of data in just a few minutes in 2008, at a time when the Pentagon was still struggling to accelerate UAV production and get more communications links to forces fighting in Iraq.

Ten years on, the Department of Defense's task is to modify existing and near-future DoD platforms to take advantage of the full potential for data fusion. By all rights, US forces should be far, far ahead in their data access and utilization. Multi-domain operations count on it.

Assigning high priority to multi-domain operations clears the way for developing the command and control to carry them out. There's no question the Service chiefs and future planners grasp the importance of adding much more resilient, data-intensive hubs to combat networks.

It won't be easy, especially since communications programs were stashed in different corners and niches of OSD on an ad hoc basis. However, American industry has provided the networking and data management tools to enhance combat networks.

"I don't have the answer," said Brig. Gen. Chance Saltzman, who led an Air Force Multi-domain functions study. "I just know we need to investigate, experiment, and explore with those concepts to get it right." [xxvi]



END NOTES

[i] Rebecca Grant, "The Rover," *Air Force Magazine*, August 2013.
[ii] Jennifer Hlad, "More BACN, Please," *Air Force Magazine Daily Report*, March 2, 2017.
[iii] "Tactical Targeting Network Technology: What You Need to Know," *Microwave Journal*, February 16, 2018.
[iv] Air Force Information Dominance Flight Plan, 2010, p. 43
[v] Ben Brimelow, "General reveals that US aircraft are being disabled in Syria," *Business Insider*, April 26, 2018.
[vi] Deputy Secretary of Defense Robert O. Work, Speech to Army War College, April 8, 2015.
[vii] Roger N. McDermott, *Russia's Electronic Warfare Capabilities to 2025*, ICDS Estonia, September 2017.
[viii] Joseph Trevithick, "Russia Jammed Phones and GPS is Massive Wargame," *The Drive*, October 17, 2017.
[ix] Megan Eckstein, "Multi-Domain Battle Concept to Increase Integration across Services Domains, USNI, October 4, 2016.
[x] Interview: Lt. Gen Ben Hodges, *Defense News*, March 26, 2015.
[xi] Stew Magnuson, "Army Scrambles to Make Command Posts Survivable," *National Defense*, December 1, 2017.
[xii] Mark Pomerlau, "Breaking Down China' C4ISR tactics," *C4ISRNet*, March 22, 2017.
[xiii] Sydney Freedberg, "HASC EW Expert: US Not prepared for Electronic Warfare vs. Russia, China" *Breaking Defense*, January 22, 2018.
[xiv] Gen. David G. Perkins, "Multi-Domain Battle: Driving Change to Win in the Future," *Military Review*, July-August 2017.
[xv] CNO John Richardson, Heritage Foundation Speech, February 1, 2018.
[xvi] Mark Pomerlau, "Marines Take Multi-Domain Battle to the Littorals," *Defense News*, September 21, 2017.
[xvii] Department of Defense Press Briefing on Fiscal Year 2019 Air Force Budget, February 12, 2018.
[xviii] Harris, et al. "A Lethal Solution for Ensuring Military Preeminence," Real Clear Defense, March 2, 2018.
[xix] Lockheed Martin press release, February 5, 2014, http://www.lockheedmartin.com/us/news/press-releases/2014/march/140307ae_lockheed-martin-demonstrates-interoperability.html
[xx] Katherine Owens, "Lockheed Enterprise Computer Connects Older Aircraft with F-35s," *Battlespace Tech*, June 8, 2017.
[xxi] Mark Daniels, May 13, 2015, "A New Class of Protected Satellite Communications," *Intelsat General*.
[xxii] AUSA, "Integrating Army Robotics and Autonomous Systems to Fight and Win," Institute of Land Warfare, July 2017.
[xxiii] Sydney Freedberg, "Joint Artificial Intelligence Center Created under DOD CIO," *Breaking Defense*, June 29, 2018.
[xxiv] Sean Kimmons, "Multi-Domain Task Force Set to Lead Pacific Pathways rotation in first overseas test," *Army News Service*, June 15, 2018.
[xxv] Kevin Woods and Thomas C. Greenwood, "Multidomain Battle: Time for a Campaign of Joint Experimentation," *JFQ 88*, 1st Quarter 2018.
[xxvi] Nov. 27, 2017 AFA Mitchell Event, Capitol Hill


WASHINGTON
SECURITY
FORUM