AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

BRIDGING THE GAP: HOW AN AIRBORNE MOBILE MESH NETWORK CAN OVERCOME SPACE VULNERABILITIES IN TOMORROW'S FIGHT

by

Travis T. Patterson, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Kelly M. Colacicco, Lieutenant Colonel, USAF

8 May 2018

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the U.S. Government, the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, *Intellectual Property—Patents, Patent Related Matters, Trademarks, and Copyrights*, it is not copyrighted, but is the property of the U.S. Government.

BIOGRAPHY

Major Travis Patterson entered the Air Force in 2006 after graduating from the United States Air Force Academy. He is a Senior Pilot with 3,300 hours—including 400 combat hours—in the U-2S, TU-2S, T-38A, and T-1A. Maj Patterson has served in a number of positions throughout his career to include Chief of Weapons and Tactics, 9th Reconnaissance Wing, Beale AFB, California, where he oversaw tactical development for the Air Force's entire high-altitude reconnaissance fleet of RQ-4 Global Hawk, and U-2S Dragon Lady aircraft. As an evaluator and operational test pilot, Maj Patterson has conducted combat ISR and peacetime Sensitive Reconnaissance Operations throughout the Pacific, Central, European, and African theaters, in support of Operations ENDURING FREEDOM, JUNIPER SHIELD, INHERENT RESOLVE, and FREEDOM'S SENTINEL. He is currently attending Air Command and Staff College, Maxwell AFB, Alabama.

ABSTRACT

The US Air Force's heavy reliance on space capabilities makes it vulnerable to potentially crippling asymmetric multi-domain attacks in the near future. While Air Force leaders have identified the importance of maintaining dominance in the space domain, their goal of attaining resilient and survivable systems in the future is not immediately attainable. Peer competitors and potential adversaries already possess several operational and developmental capabilities, which place critical US space assets on the losing side of a cost-exchange battle. An option to mitigate many of these risks exists in an airborne mobile-mesh network hosted initially by the Air Force's high-altitude ISR platforms.

U-2S Dragon Lady and RQ-4B Global Hawk aircraft provide an excellent foundation upon which the Air Force can field and operationalize an airborne mobile-mesh network in the battlespace to augment critical space capabilities. Compared to the extreme cost of vulnerable satellites, such a network would not only be cost-efficient, but could also provide improved resilient capabilities to the Joint Force without requiring drastic changes in operational tactics, techniques, and procedures. This research proposes that the US Air Force rapidly field a mobile-mesh network using existing technology and platforms, and then continue to build the network and processing capabilities over the course of the next decade. The Air Force's vulnerabilities in space have the potential to impact combat operations in every domain across the globe. It is time to capitalize upon research and investments already made, and make the first step toward a truly connected and networked force.

TABLE OF CONTENTS

LIST OF FIGURES vi

LIST OF ACRONYMS AND ABBREVIATIONS vii

Introduction 1

Scope of the Problem 5

Understanding Mesh Networks 8

Function and Viability of an Airborne Mesh Network 12

Advantages of High-Altitude Platforms 14

Basic Equipment and Necessary Technologies 18

Mission Assurance and Cyber Protection 23

The Art of the Possible: Today and Tomorrow 26

Recommendations 35

Conclusion 38

NOTES 39

BIBLIOGRAPHY 47

LIST OF FIGURES

Figure 1 – Current Dataflow and Vulnerabilities.. 9

Figure 2 - Hierarchical Network Topology 11

Figure 3 - Mesh Network Topology (Unlimited Connectivity) 11

Figure 4 - Mesh Network Topology (Limited Connectivity)... 11

Figure 5 - Line-Of-Sight Advantage of High-Altitude Platforms.. 16

Figure 6 - U-2S Hosting LLAN During Project Hunter Experimentation 19

Figure 7 - Example of a High-Altitude "Data Bridge" 30

Figure 8 - Example Network in 5 Years.. 32

Figure 9 - Example Future Network Using Chameleon 37

LIST OF ACRONYMS AND ABBREVIATIONS

A2AD	Anti-Access Area-Denial
AESA	Active Electronically Scanned Array
AFRL	Air Force Research Laboratory
AJ	Anti-Jam
ALE	Automatic Link Establishment
AOR	Area of Responsibility
ASARS	Advanced Synthetic Aperture Radar System
ASAT	Anti-Satellite
ARGOS	Advanced Reconnaissance Geospatial Orbital System
ATR	Automatic Target Recognition
BLOS	Beyond-Line-of-Sight
BMC2	Battle Management Command and Control
C4ISR	Command, Control, Communication, Computers, Intelligence, Surveillance, and Reconnaissance
COP	Common Operating Picture
COSS	Celestial Object Sighting System
DCGS	Distributed Common Ground System
DE	Directed Energy
DOD	Department of Defense
DODIN	Department of Defense Information Network
ECCT	Enterprise Capability Collaboration Team
EM	Electromagnetic
EWS	Electronic Warfare System
FMV	Full Motion Video
GPS	Global Positioning System
HF	High Frequency
I&W	Indication and Warning
IA	Information Assurance
IFDL	Intra-Flight Data Link
IMINT	Imagery Intelligence
IP	Internet Protocol
ISR	Intelligence, Surveillance, and Reconnaissance
JUON	Joint Urgent Operational Need
LEO	Low Earth Orbit
LLAN	Low Probability of Intercept, Low Probability of Detection, Anti-Jam Network
LO	Low Observable
LOS	Line-of-Sight
LPD	Low Probability of Detection

LPI	Low Probability of Intercept
LRASM	Long Range Anti-Ship Missile
MADL	Multifunction Advanced Data Link
MANET	Mobile Ad Hoc Network
MIT	Massachusetts Institute of Technology
MLS	Multi-Level Security
MMN	Mobile Mesh Network
MSL	Mean Sea Level
OA	Open Architecture
OMS	Open Mission Systems
OODA	Observe, Orient, Decide, Act
OPIR	Overhead Persistent InfraRed
PCA	Penetrating Counter-Air
PNT	Precision Navigation and Timing
PRC	People’s Republic of China
RF	Radiofrequency
SAR	Synthetic Aperture Radar
SATCOM	Satellite Communication
SDA	Software Defined Antenna
SDR	Software Defined Radio
SIGINT	Signals Intelligence
SWaP	Size, Weight, and Power
TTPs	Tactics, Techniques, and Procedures
UAS	Unmanned Aerial Systems
UHF	Ultra High Frequency
USAF	United States Air Force

Introduction

> Air and Space superiority is not America's birthright, we earned it the hard way, and we are not going to give it up without a fight…Since 1954 the United States Air Force has been the lead service for space. Up to about 10 years ago, space was a benign environment. Our potential adversaries know how much we depend upon it; they understand the advantages that we gain in space. We must expect space to be a contested domain in any future high-end conflict. We must seek to deter attacks on our satellites, and if deterrence fails, our space systems must be resilient so we can take a punch and fight back.
>
> –Hon. Dr. Heather A. Wilson, Secretary of the Air Force[1]

Throughout history, generals across the globe have sought to obtain and fight from the high ground whenever possible. From Sun Tzu to Alexander, and Thucydides to U. S. Grant, history's most successful tacticians and battlefield leaders have understood that even a numerically inferior force can command a battlefield if it occupies the right position. In the 20th century, those forces able to obtain and maintain superiority in the air domain dominated the battlespace below, because "as protectors of the high ground, you unleash enormous capabilities on the low ground."[2] Now, in the 21st century, the high ground has ascended even further into the space domain, which not only commands the battlespace below by virtue of physical location, but also from a multi-dimensional aspect as it enhances every function of the other domains it oversees. Modern military leaders are well aware of the critical capabilities that space provides to the different domains, as well as the serious challenges their forces would face if forced to risk a fight without them. Specifically, United States Air Force (USAF) Chief of Staff, Gen David Goldfein recognized that, "space is the ultimate high ground…[the USAF] owns space, and [it] owns space on the obligation that [it] has to be able to ensure space superiority in the future, to hold the ultimate high ground."[3]

Unfortunately, occupying the ultimate high ground comes at tremendous cost, and for the past several decades, American space forces have enjoyed relative supremacy based largely on the fact that no other competitors were technologically or financially able to present a competitive threat. At present, “the space domain is undergoing a significant set of changes… [as] a growing number of countries and commercial actors are getting involved in space.”[4] Rapid advancements and increases in technological development have led to smaller and cheaper satellites, and commercial competition has driven down the cost of placing them into orbit. As space becomes ever more critical for national security as well as commercial and economic success, potential adversaries will certainly continue to develop the ways and means to disrupt and exploit any potential weakness in the domain. Most traditional space assets are large, costly, and difficult to defend against the myriad of cheaper and more agile counterspace capabilities available to potential adversaries across the globe.[5]

If diplomacy and deterrence broke down within the next 15 years to the extent that the United States found itself in a war with a peer adversary, we would rapidly discover that as a whole, our existing space constellation is unprepared, inadequately defended, and vulnerable to multi-dimensional and multi-domain attacks. Such asymmetric attacks against our space assets could have dramatic consequences to the Joint Force’s lethality and ripple throughout every combat domain. Coalition and Joint Forces reliant on the “force multiplying” assistance and unwavering reliability of space services will experience degradation of position, navigation, and timing (PNT), satellite-hosted communications, and airborne and overhead Intelligence, Surveillance, and Reconnaissance (ISR) collection and dissemination. Such degradation can range from nuisance interruptions in Ultra High Frequency (UHF) Satellite Communications (SATCOM) and Link-16 reliability caused by terrestrial and aerial jamming, to complete denial of critical indications and warning (I&W) and weapons guidance through kinetic engagement or deliberate spoofing and jamming of the Overhead Persistent Infrared (OPIR) and Global Positioning System (GPS) constellations.[6]

Identifying such vulnerabilities is not to suggest that US space forces and assets are incompetent, ill designed, or not somewhat resilient; only that they are asymmetrically vulnerable and on the losing end of a cost-exchange battle with a determined enemy. Nor is it likely that even a highly motivated and well-armed adversary could negate America's entire spaceborne advantage all at once, as there are simply too many platforms dispersed across multiple orbits to engage them all. However, while numbers and orbital variation may offer some minor assurance that America's huge capital investment in exquisite monolithic satellites is not a waste, the strategic advantage belongs to the adversary who is able to disrupt and destroy key capabilities for pennies on the dollar.[7] Furthermore, an enemy need not engage every satellite to seriously hinder US capabilities in a region, they only need to kinetically engage certain key nodes (both orbital and terrestrial) and layer electromagnetic (EM) jamming throughout the theater. There is no way to know exactly what an adversary would target, and it is therefore impossible for the United States to guarantee any specific capability or functionality to its forces once the enemy seizes the offensive initiative in space.

Leaders and decision makers in the United States are neither blind to these threats nor sitting complacently as America's advantage wanes.[8] They are actually setting ambitious goals to expedite development and operationalization of newer resilient and survivable systems, capitalizing on industry partners as well as Department of Defense (DOD) ideas and technologies to address the mounting threat to our glaringly vulnerable constellations.[9] Unfortunately, "hardening" and replacing the various individual assets or constellations supporting the global Joint Force is neither cheap nor expedient. Potential adversaries have already seized the initiative in this regard by fielding multi-domain capabilities capable of degrading and denying American space superiority while retaining a cost-exchange battle advantage. Therefore, in order to overcome these near-term challenges and maintain information dominance at the speed and scale of modern warfare, the DOD must rapidly develop and employ an airborne mobile mesh network (MMN) as a resilient and redundant solution to overcome some of the vulnerabilities inherent in the current space constellation. My research focuses on already existent and some emerging developmental technology, explores the potential functionality of such a network, and suggests high-altitude ISR platforms as the most capable candidates for an initial MMN fielding.[10] By combining existing and emerging technology onboard its modular fleet of high-altitude ISR platforms, the USAF can provide an agile and adaptable option for resilient command, control, communications, computers, and ISR (C4ISR) dataflow in a degraded or denied space environment.

Scope of the Problem

> Largely since 1991, our Air Force has been focused on integrating space capabilities into theater operations, and we've done so in a relatively benign domain; there hasn't been a threat to really be concerned about. This integration has provided us incredible advantage and we see this every day playing out in the theater today. But that's no longer a given…space superiority is no longer a birthright, and we feel in the future we're going to have to fight for that space superiority, if we were to get into a high end fight.
>
> –Gen John W. Raymond, Commander, Air Force Space Command[11]

The Air Force Future Operating Concept describes a highly dynamic multi-domain force in the year 2035 that operates "robust, resilient capabilities provided through cyberspace or space assets… [which] reduce reliance on traditional air platforms to product certain effects."[12] The space assets providing this "operational agility" will employ robust "mission assurance capabilities" to ensure unfettered functionality in that increasingly contested and potentially degraded domain.[13] Unfortunately, the Air Force of 2018 relies on a space network that is neither defensively robust nor overly resilient when compared to the array of advanced threats our peer adversaries are able to employ against it.

A year after the successful 2014 Chinese anti-satellite (ASAT) weapon test, General John Raymond stated, "soon every satellite in every orbit will be able to be held at risk."[14] With those few words, the Commander of Air Force Space Command summed up the enormous problem set facing the USAF and its Joint partners. Both the People's Republic of China (PRC) and Russian Federation maintain ASAT capabilities that can disrupt or deny US space assets across multiple orbits. Particularly alarming is the PRC's progress across the spectrum of ASAT technologies, to include direct ascent, co-orbital, and directed energy (DE) weapons.[15] China may have up to three different development programs underway for direct-ascent ASAT capabilities alone, with programmatic maturity, ranging from purely experimental or developmental, to operationally fielded mobile launchers.[16] Even back in 1985 as a research fellow at the Massachusetts Institute of Technology (MIT) Center for International Studies, future Secretary of Defense Ashton B. Carter recognized the threat of ASAT weapons, and the difficulty defending against a deliberate attack.[17] While the Air Force of 2035 may enjoy “defensive space control operations [which] increase resilience of space systems and architectures, and improve reconstitution capabilities,” we are still over a decade away from fielding such technologies in an operationally relevant quality and quantity.[18]

The threat to US space assets is not only a kinetic one propagated by other great powers, but a multi-domain problem stemming from state and non-state actors alike. Unlike the threat of nuclear proliferation, which maintains the highest scrutiny of the world’s intelligence communities, technological distribution and non-kinetic threats are much harder to track, deter, and discourage. For example, the Russian Federation providing “Krasukha-4” synthetic aperture radar (SAR) and “Zhitel” GPS jammers to a nation like Syria would not likely generate quite the international backlash that providing nuclear weapons to Iran might.[19] Potentially hostile actors increasingly threaten American satellites as they field “dazzling, jamming, kinetic impacts, and cyber means” through internal development or international acquisition.[20] The crucial but immovable ground segments of the space infrastructure are also vulnerable to terrorist and cyber-attacks. However, “perhaps the greatest fear is that any attack could provoke a chain reaction of collisions that renders entire orbits useless, known as the *Kessler Syndrome*.”[21]

Rapid commercialization of the space domain and subsequent decreases in the cost of reaching orbit will also threaten American military dominance. The problem does not necessarily stem from the possibility of hostile actors employing their own satellites, but from the number of objects actually in orbit. Just as congestion in the air presents a threat to aircraft, so too will the influx of new satellites, carried into space by Falcon 9 (SpaceX), New Shepard (Blue Origin), and Electron (Rocket Lab) rockets, threaten orbits already at “critical density.”[22] The congested space environment of the near future will not only be a result of commercial entities, but also of the DOD itself, which appears increasingly interested in the potential of SmallSats and CubeSats for military purposes.[23] For example, the *Blue Horizons* program under the USAF Center for Strategy and Technology is proposing a persistent and resilient command and control architecture via a space-based mega-constellation of CubeSats. Their Advanced Reconnaissance Geospatial Orbital System (ARGOS) concept seeks to complicate the adversary’s targeting equation and providing a numerical resiliency to spaceborne capabilities.

CubeSats will certainly provide critical and unique capabilities in the near future, at a far more advantageous cost and level of resiliency than the current billion dollar monoliths in service. Facing a CubeSat mega-constellation, an adversary would have a vastly larger set of targets, and much like a mesh network, would be unable to disrupt the constellation’s capabilities by targeting only a few satellites. Kinetically, a large constellation of smaller, cheaper satellites shifts the cost-exchange battle to a more favorable balance as the aggressor must choose to expend valuable ASAT capabilities against swarms of shoebox-sized targets. Instead, the adversary would likely select non-kinetic means to disrupt a CubeSat constellation, and employ DE and EM warfare to degrade or destroy the small satellites. No matter which counterspace option an aggressor selects (kinetic or non-kinetic), the disabled or destroyed CubeSats and their replacements bring all of Low Earth Orbit (LEO) even closer to the *Kessler Effect*.[24]

Understanding Mesh Networks

> We see a significant opportunity to drive a digital transformation in C4ISR…The open systems architecture really being foundational…It will be key to quickly evolving technology, ensuring operability, and ultimately affordability, that there be a common architecture across the platforms… Another opportunity around digitally enabled multi-function capabilities allowing the same hardware to be programmed with multiple capabilities, and be able to switch those capabilities as needed.
>
> –Mr. Bryan Lima, Program Director for Manned C2 ISR, Northrop Grumman[25]

Before exploring the military potential of an airborne MMN, it is important to clarify what a MMN actually is, and how it functions. Broadly speaking, a "traditional" network such as the Internet as a whole or the Department of Defense Information Network (DODIN), is "based on a few centralized access points or internet service providers," with nodes connecting to each other by first passing through a "central authority or centralized organization."[26] This hierarchical structure is vulnerable to various types of network (cyber) threats, and susceptible to single points of failure at "bottlenecks," especially during periods of high demand. Conceptually, this is very similar to the dataflow architecture of a modern ISR platform. For example, an RQ-4B may collect imagery (IMINT) and signals (SIGINT) intelligence with its specialized sensors, but must push that data off board for processing, exploitation, and dissemination. The data must pass through a commercial Ku satellite to its corresponding ground site, then through fiber connections and eventually to the Air Force Distributed Common Ground System (DCGS) for processing, exploitation, and further dissemination.

This type of dataflow has proven sufficient during permissive operations; however, several problems emerge in a contested environment. The data pathways of today's ISR enterprise are simply a largescale hierarchical network, vulnerable to the same risk of targeted attacks as any other linear system. Figure 1 demonstrates how an adversary can employ kinetic weapons against key nodes such as satellites, their ground sites, and even DCGS facilities (outlined in red dashes), employ non-kinetic effects in the form of cyber-attacks against infrastructure (green clouds outlined in red), or EM spectrum warfare in theater against datalinks, communications, and ISR sensors (lightning bolts). An attack on one of these critical nodes can cripple the broader network, potentially rendering numerous C2ISR functions ineffective throughout an entire AOR. A truly determined adversary will likely layer kinetic and non-kinetic effects to overwhelm any amount of limited redundancy built into this hierarchical system. These are the types of "legacy ISR and support infrastructures… now failing to help commanders and war fighters meet essential goals" as they plan for "great power" conflicts in an increasingly unstable world. [27]

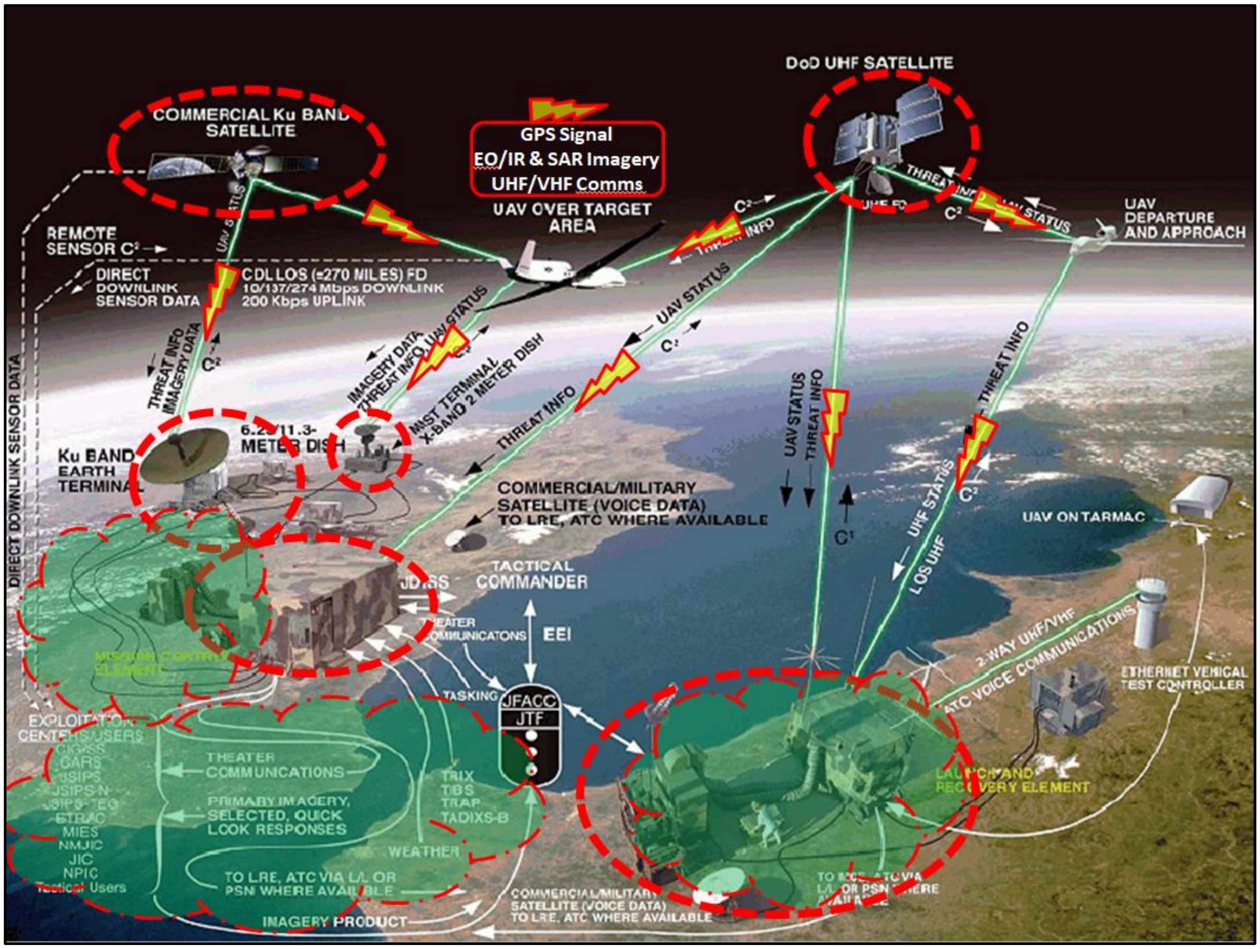
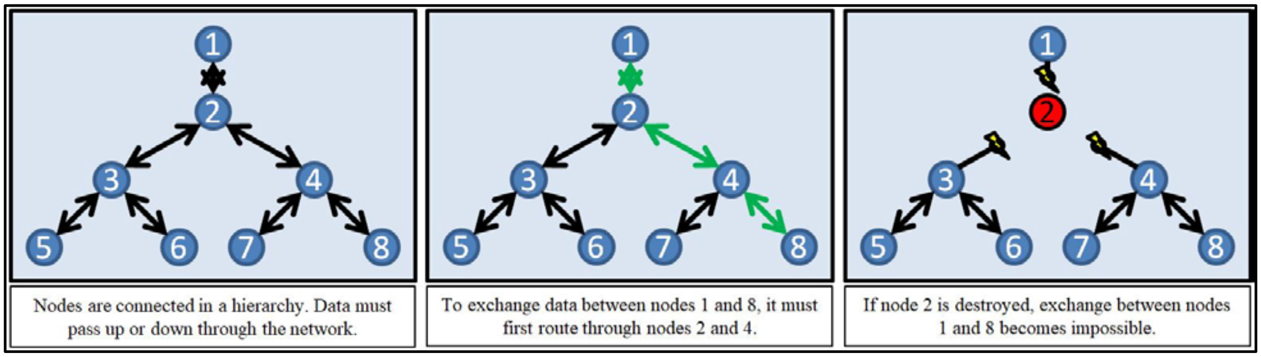


Figure 1 – Current Dataflow and Vulnerabilities[28]

A basic mesh network is a “topology in which the infrastructure nodes connect directly, dynamically and non-hierarchically to as many other nodes as possible and cooperate with one another to efficiently route data from/to clients.”[29] This is a much more versatile network when compared to the linear structure of a hierarchical topology, where large sections of a network rely on single points of potential failure (see Figure 2). When nodes in a mesh network connect wirelessly, they become a mobile ad hoc network (MANET) which is able to “automatically reconfigure [itself] according to the availability and proximity of bandwidth, storage, and so on…dynamic connections between nodes enable packets to use multiple routes to travel through the network, which makes these networks more robust” (see Figure 3).[30] Since these networks are “continuously self-configuring” and “infrastructure-less,” the only way to disable the entire network is to destroy every node (see Figure 4).[31] Without a central administrator to control data input and output, it is incumbent upon the individual nodes to possess some level of processing power. The amount of processing, and the associated algorithms to prioritize and direct dataflow between nodes and throughout a given network is beyond the scope of this proposal, but the concept is not new to academia.[32]

Some commercial entities have already identified the advantages of MANET and MMN capabilities both on the ground and in the air.[33] In 1998, *Airborne Wireless Network* patented technologies necessary to establish a “Wholesale Carrier Network,” using commercial aircraft across the globe as “mini-satellites.”[34] Their goal is to create a virtual airborne “worldwide web” which provides “connectivity for worldwide broadband carrier services,” leveraging the multiple pathways of a massive meshed network.[35] *Airborne Wireless Network* will also capitalize on another extremely advantageous aspect of mesh networks: the ease of updating, upgrading, and servicing the network itself. “As new software becomes available, the system can be easily updated. When new and more efficient data-transmission technologies emerge, [*Airborne Wireless Network*'s] system can be as easy as replacing a single module, and the system is ready for 'the future.' The Network is never obsolete. Satellite technology, on the other hand, in most cases, has already been surpassed by the time a satellite is launched."[36]

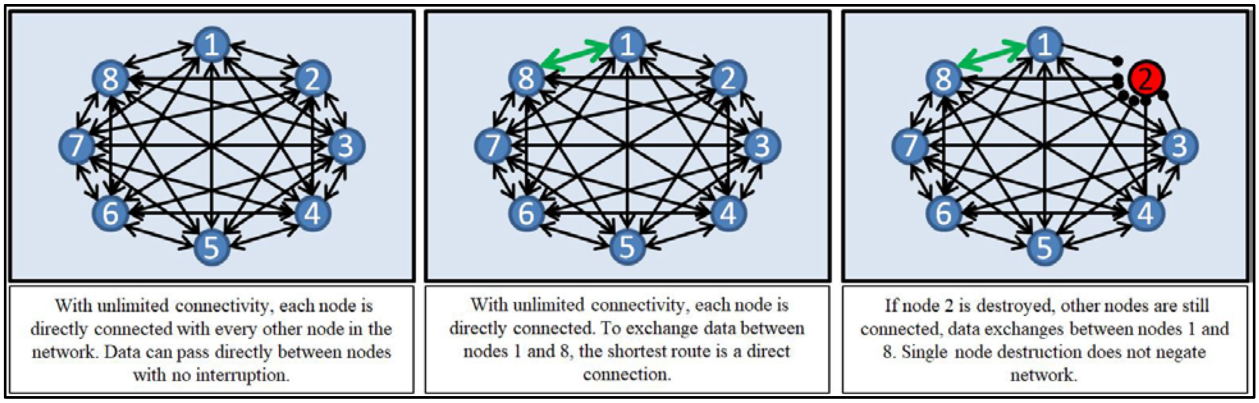


Nodes are connected in a hierarchy. Data must pass up or down through the network.

To exchange data between nodes 1 and 8, it must first route through nodes 2 and 4.

If node 2 is destroyed, exchange between nodes 1 and 8 becomes impossible.

Figure 2 - Hierarchical Network Topology

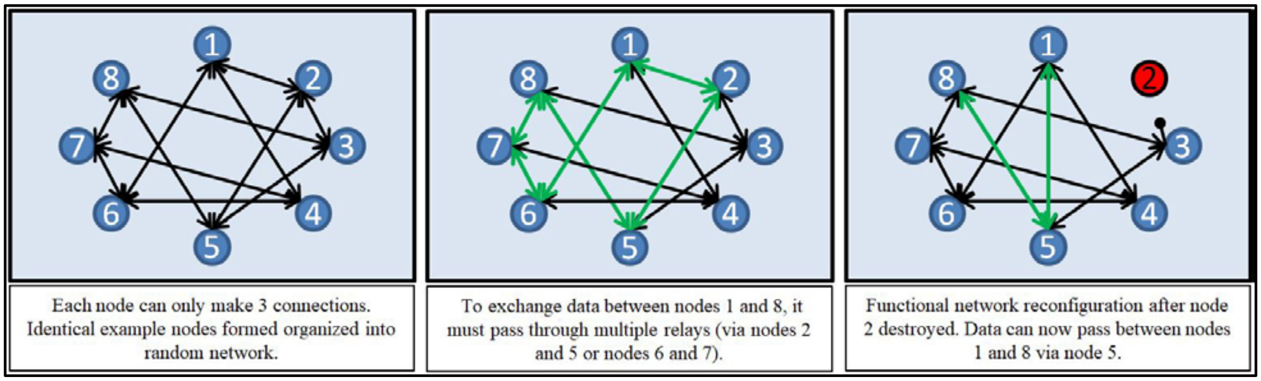


With unlimited connectivity, each node is directly connected with every other node in the network. Data can pass directly between nodes with no interruption.

With unlimited connectivity, each node is directly connected. To exchange data between nodes 1 and 8, the shortest route is a direct connection.

If node 2 is destroyed, other nodes are still connected, data exchanges between nodes 1 and 8. Single node destruction does not negate network.

Figure 3 - Mesh Network Topology (Unlimited Connectivity)



Each node can only make 3 connections. Identical example nodes formed organized into random network.

To exchange data between nodes 1 and 8, it must pass through multiple relays (via nodes 2 and 5 or nodes 6 and 7).

Functional network reconfiguration after node 2 destroyed. Data can now pass between nodes 1 and 8 via node 5.

Figure 4 - Mesh Network Topology (Limited Connectivity)

Function and Viability of an Airborne Mesh Network

> The answer really should start out with “what data do you want off the platform? Where do you want it to go? Who do you want to get it? What are they going to do with it?” If you can just answer some of those questions… then it starts to fill in the gaps of “what’s the best datalink for that situation in what area?” Because you can get a datalink out there that does anything you need.
>
> – Lt Gen Charles R. Davis, USAF (Ret.), L3 Technologies.[37]

Understanding that our extremely expensive national systems in every orbit are vulnerable to non-kinetic disruption or kinetic destruction, the USAF must explore a solution outside of the space domain to ensure continued C2 and ISR dataflow in the event of near-term conflict with a peer competitor. An airborne MMN is a promising option available to the USAF and its Joint partners to overcome some of the aforementioned limitations. The benefits of a networked approach to warfare include resiliency, disaggregation of systems and sensors, and scalability to suit numerous problem sets.[38] A network of all types of aircraft and sensors with the ability to share data in a common language, would not only improve the quality of intelligence in the network’s region, but would also enable reliable means of communication to any available node in the network. Furthermore, as the number of participating nodes in a single network increases, the available pathways for dataflow also increase. This type of interconnectivity serves not only the needs of the specific network, but also the DoD’s broader Network Services 2020 plan which seeks to enable a “cohesive global network that will consist of all types of [nodes], with voice, video and data transmitted around the world on a 100-gigabit-per-second backbone.”[39]

In order to meet the needs of warfighters and decision makers in the modern battlespace, a network must be survivable in the face of EM jamming and disruption. This requires the waveform connecting all of the nodes to maintain intelligent agility in the face of various jamming techniques, and operate in modes not susceptible to enemy detection. It must be selfforming as nodes enter and leave the network, and it must be self-healing in the event of equipment or software malfunction, or node destruction. In fact, an airborne MMN must meet all of the requirements of a “combat cloud.”[40] It must enable “automatic linking, seamless data transfer capabilities, while being reliable, secure, and jam proof.”[41] This concept would transform the current “industrial age” ISR dataflow architecture into an “information age” system-of-systems enterprise, in which a common data language would agnostically connect and transfer sensor and platform information. “The idea is that a sensor can come online to a network, register and communicate its capabilities to the network and, in turn, other assets and sensors on the network can subscribe to the types of information they want or don’t want – basically like a filter…Now, you have this fundamental architecture enabling sensors to not only recognize the systems they want to interact with but also broker the information exchanges.”[42]

Advantages of High-Altitude Platforms

> First and foremost, ISR is all about decision advantage. Decision advantage in air, space, cyber, surface and subsurface. I.e. Multi-domain, multi-INT, and access in a multi-security environment. That's really what we have to do. I've coined the phrase and I've talked about fusion warfare for several years now, and really fusion warfare is decision advantage at speed and scale, at a time and place of our choosing, to create the desired effect that we want inside of the adversary's OODA loop. And so I really believe as we look to the future, those who are the fastest at collecting, correlating, fusing, analyzing, transporting the right decision quality information, across multiple domains for the right decision maker, to generate effects across both physical and geopolitical space, is who is going to win the next conflict.
>
> – Lt Gen VeraLinn Jamieson, Deputy Chief of Staff for ISR, US Air Force[43]

High-altitude airborne platforms offer a unique set of capabilities in building an operational airborne MMN. Platforms such as the U-2S and RQ-4B offer extreme line-of-sight (LOS) advantages over other airborne systems, making them an ideal "backbone" since they can provide coverage over vast areas of the battlespace. If a specific waveform and radio were not limited by any factor other than LOS, two nodes operating at an altitude of 65,000 feet would be able to connect at a distance greater than 540 nautical miles, with each individual node able to cover an area of airspace more than 915,800 square miles.[44] To put that kind of range in perspective, three high-altitude nodes operating in the Asia-Pacific region could create a network backbone stretching 2,000 nautical miles, from the southern tip of Vietnam and the Spratly Islands all the way to the Yellow Sea and Sea of Japan. Furthermore, both the U-2S and RQ-4B already conduct operations across the globe, making them available and in-place for rapid network development.

Additional advantages to employing high-altitude platforms as the initial nodes in an operational MMN are their long ranges and loiter times. For example, the RQ-4B can travel a distance of 12,300 nautical miles over the course of a 34 hour mission, while a manned U-2S can cover nearly 7,000 nautical miles over a 12 hour mission.[45,46] In an uncontested environment, such loiter time provides extended coverage over a vast area of the battlespace. In a contested environment, the LOS advantage could keep high-altitude platforms out of range of even the most advanced threat systems and still provide overlapping coverage in a specific area of operations (AOR). Moreover, high-altitude platforms can travel extremely long distances, which alleviates burdening high-demand tanker assets for aerial refueling, and enables them to launch (and recover) from bases out of range from immediate kinetic threats.

Furthermore, the increased standoff ranges and high operating altitudes of the U-2S and RQ-4B offer superior LOS advantages to satellite relays, which may be outside the range of some adversary ASAT capabilities, especially those requiring a direct LOS to target the satellite. If an enemy jammer targeted a commercial or military communication satellite associated with a high-altitude platform, it may be possible to switch relays and communicate with a different satellite orbiting out of jamming range. For example, a platform operating above 60,000 feet is able to establish LOS communications with a satellite relay outside the field of view of a platform at sea-level (see Figure 5). The ability to look beyond the curve of the earth compared to a ground-based jammer could provide an additional option for relaying data using a beyond line-of-sight (BLOS) architecture in and out of a contested battlespace.[47]

RQ-4 Block 30 unmanned aerial systems (UAS) equipped with the modular ISR payload adapter and the inherently modular U-2S further strengthen the case for high-altitude network nodes with their ease of carrying new or additional equipment. The U-2S's 5,000-pound payload and configurable airframe and super-pods, combined with its 45-kVA generator, can easily host the antennas and radios necessary to serve as a MMN node. In 2017, the U-2S actually flew experimental MMN technology in a series of tests and exercises, with no adverse impact to normal flight operations. These flights demonstrated the relative speed and ease with which the platform can host such technology and still accomplish its assigned missions.[48] Further plans to incorporate an *AgilePod* to the U-2S in 2018 enhance not only the individual platform's ISR capabilities, but also the potential for new processing power of the MMN as a whole. *AgilePod* is an adaptable, rapidly reconfigurable, open architecture external pod that can house any number of sensors, antennas, or processors, making it an ideal option for an MMN node with "size, weight, and power" (SWaP) availability.[49] Such modifications to the U-2S come with relatively low risk and substantially lower cost when compared to similar capabilities incorporated onto other "air-breathing" platforms; compared to orbital alternatives, the cost savings is substantial.

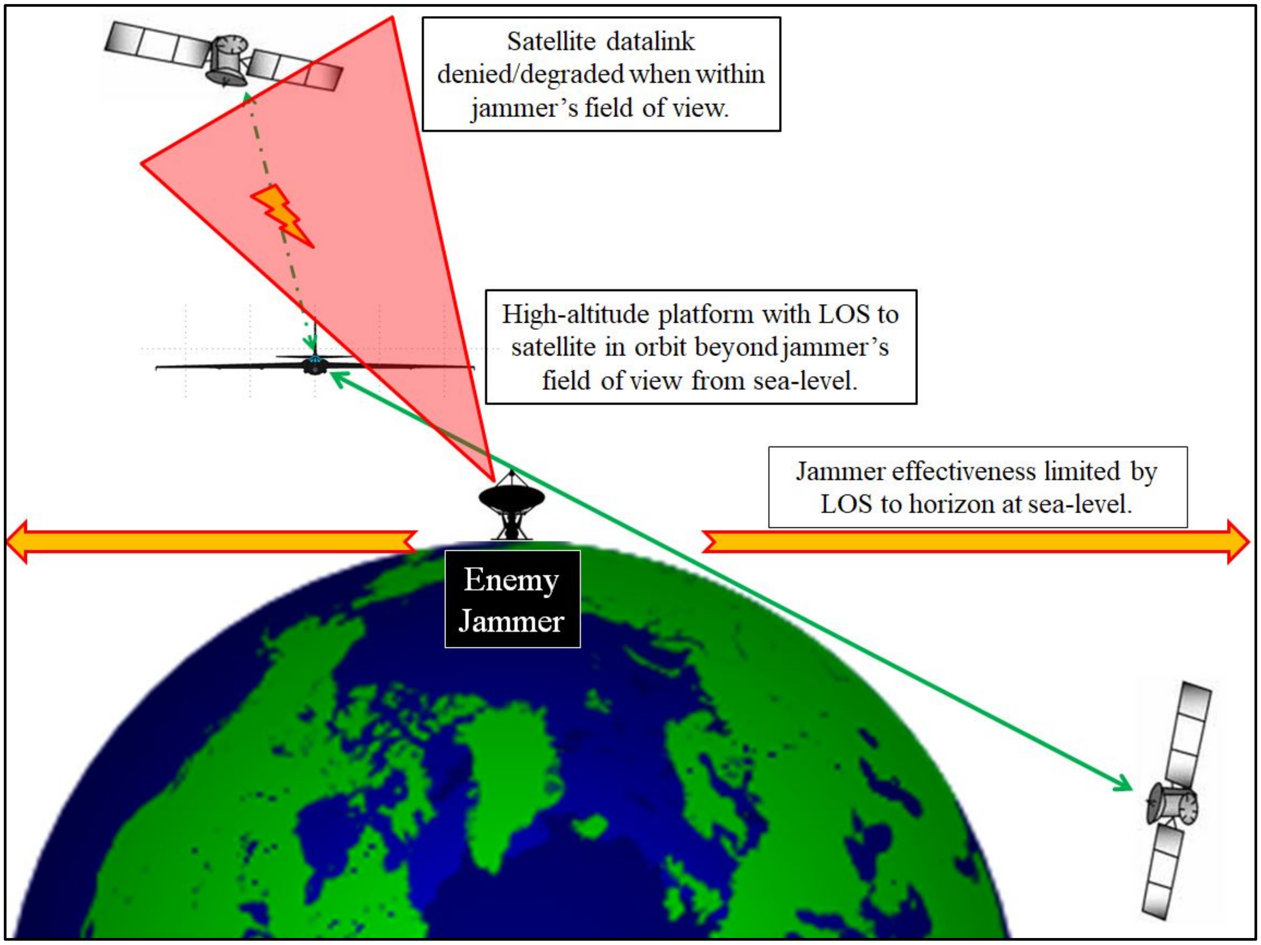

Satellite datalink denied/degraded when within jammer's field of view.
High-altitude platform with LOS to satellite in orbit beyond jammer's field of view from sea-level.
Jammer effectiveness limited by LOS to horizon at sea-level.
Enemy Jammer

Figure 5 - Line-Of-Sight Advantage of High-Altitude Platforms[50]

Finally, these platforms enjoy a certain amount of survivability by virtue of their high operational altitudes. The RQ-4B is not highly maneuverable, nor does it employ a defensive system, however its high altitude and long range allow it to operate outside of many threat rings and still accomplish its multi-INT ISR missions. As an unmanned platform, it can operate in locations or execute missions which are either too great in distance or duration to reach, or too important but too dangerous for manned platforms such as the U-2S. Alternatively, the U-2S employs a highly capable advanced electronic warfare system (EWS) and benefits from high maneuverability at operational altitude when necessary. Its faster airspeed, defensive system, and maneuverability make it a more survivable network node than the longer endurance unmanned RQ-4, but does require a human-in-the-loop, which comes with some risk.

Basic Equipment and Necessary Technologies

Central to an airborne MMN is the technology onboard the nodes (to include radios, antennas, and processors), and the waveform which links them. To meet the timeframe required in this research and provide connectivity in a space denied environment, the USAF should leverage already existing technologies. The Low Probability of Detection (LPD), Low Probability of Intercept (LPI), Anti-Jam (AJ) Network (LLAN) project addressed a number of DoD vulnerabilities and capability gaps, beginning in 2014.[51] It sought to provide interoperability between disparate platforms, to include safely bridging 5th to 5th and 5th to 4th generation communication gaps. Additionally, the LLAN project aimed to provide geolocation to networked systems in the event of GPS denial or degradation.[52]

The LLAN project employed a new anti-access area-denial (A2AD) waveform called "Chameleon" in a series of realistic tests and exercises, in various high-intensity jamming environments, with extremely positive results. "Chameleon can seamlessly change many of its waveform and networking characteristics over a wide dynamic range (without dropping bits or significantly interrupting the transmission), so it offers the ability to operate unpredictably" within the contested EM spectrum of an A2AD environment.[53] This capability exists today, has flown on U-2S and other aircraft, and successfully demonstrated excellent performance in highly dynamic and contested operating environments.[54] For example, a U-2S successfully hosted a LLAN payload as part of the Project Hunter experimentation series, culminating at Exercise NORTHERN EDGE in 2017 (see Figure 6). The LLAN report summarized the project's results as "likely the most capable A2AD communications waveform in the world."[55]

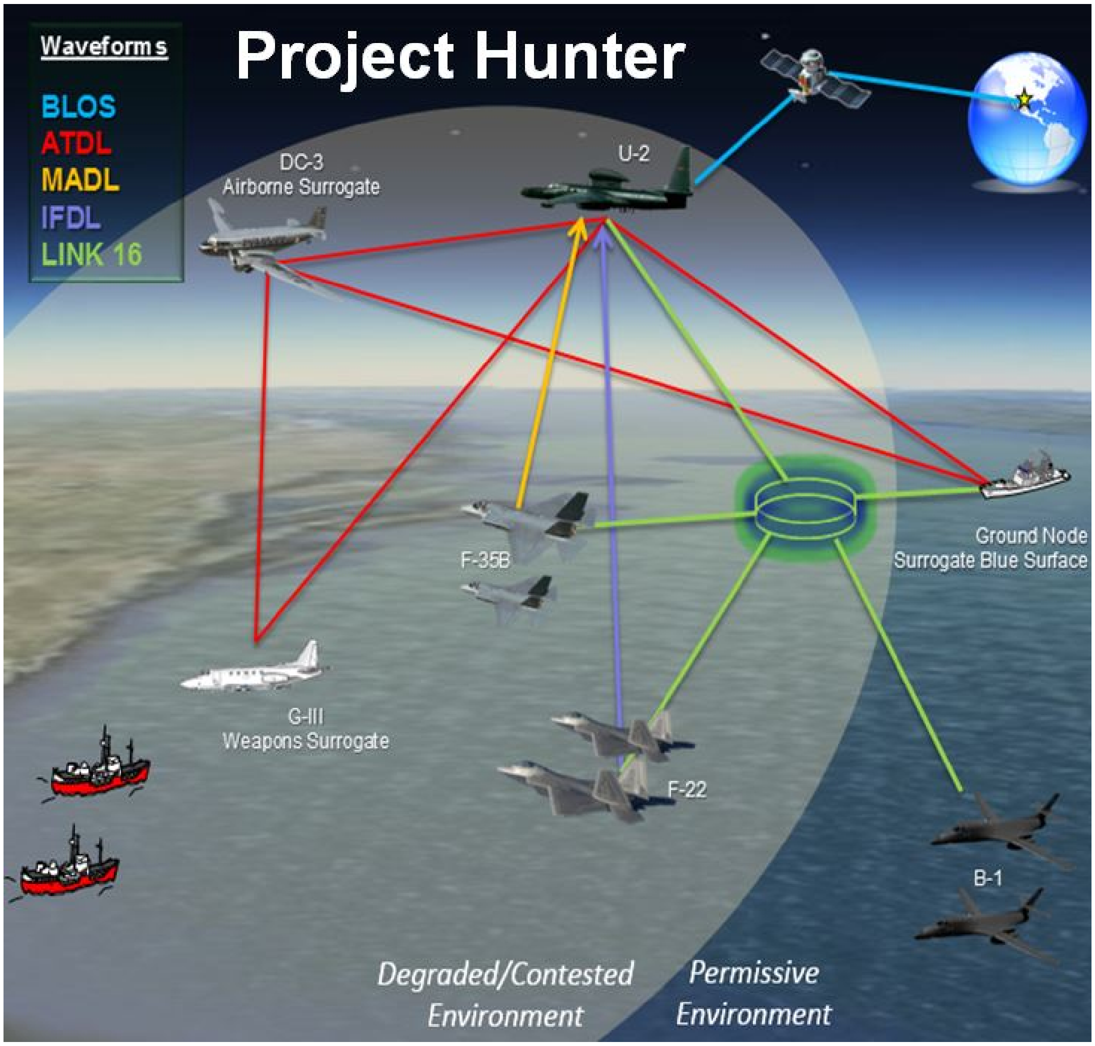


Figure 6 - U-2S Hosting LLAN During Project Hunter Experimentation

The SDR mentioned in the LLAN report is another crucial aspect of a fully capable MMN; it is the effectual "heart" of an induvial node, generating and adapting the waveform as necessary to maintain connection and distribute and receive data. Traditional hardware-based radios require physical intervention to modify their performance in transmitting and receiving radio frequency (RF), thus offering minimal flexibility in supporting multiple waveform standards necessary in an agile network.[56] Those familiar with older High Frequency (HF) Automatic Link Establishment (ALE) systems on aircraft and ships will likely notice an immediate connection to a MMN. An ALE system works by automatically optimizing the connectivity between two stations (or nodes) across a set of predetermined HF frequencies in real time, "while avoiding guesswork, beacon listening, and complicated HF prediction charts."[57] In a MMN, each SDR on each node functions in a very similar way, except it communicates with multiple other "multi-mode, multi-band and/or multi-functional" SDRs in the network.[58]

Similar to *Airborne Wireless Network's* commercial aircraft internet network, an SDR enables new features and capabilities to join existing infrastructures without expensive or expansive maintenance or downtime, thus "future-proofing" the network. In a situation where multiple nodes will be joining a MANET from numerous basing locations (some perhaps more remote than others and thus unable to provide complete tech support to host platforms), "remote software downloads, through which capacity can be increased, capability upgrades can be activated and new…features can be inserted."[59] These remote updates become critically important in an "austere basing" scenario, or when an encryption key update or change is required during actual mission execution. Finally, SDR technology is necessary to make the functionality leap from "adaptive" and "cognitive" to "intelligent" radios, which respectively modify their own internal operating parameters, monitor and optimize their own states to counter environmental factors, and perform machine learning improve the ways it adapts to internal performance changes and external environmental factors.[60]

The final hardware component necessary to truly capitalize on a SDR-enabled network is the transmit antenna. Antenna selection is crucial, and quite possibly one of the most difficult and expensive aspects of a proposed MMN because different nodes (aircraft, surface vessels, ground units, etc.) have different requirements and limitations. Furthermore, different antenna types provide different capabilities. For example, omnidirectional antennas can transmit and receive less data over smaller ranges than a similarly powered directional antenna, but are more efficient when building a network since it can create multiple links. Alternatively, a directional antenna provides the highest data rates and strongest connections between nodes at longer ranges (up to 10 times farther than an omnidirectional system), but is limited to the number of nodes it can reach at a given time.[61] In 2017, Rockwell Collins demonstrated a new directional communication link which "can point up to eight directions at the same time while simultaneously receiving a variety of signals," while still significantly reducing the size and weight of the technology.[62]

For the high-altitude aircraft this research suggests, antenna selection is relatively simple due to the minimal SWaP restrictions on the platforms and the lack of low observable (LO) requirements. As "backbone" nodes in a MMN, the U-2S and RQ-4B can each host arrays of multiple antennas, both omnidirectional and directional. Such variety will enable the "backbone" nodes to not only maintain omnidirectional coverage across a large area to rapidly generate an initial network and facilitate broad connectivity for other nodes, but also bridge long distances with high data rates to ensure complete coverage and reachback within the desired AOR. These antennas can be dedicated to specific bands of the RF spectrum, or they could be multi-layered Software Defined Antennas (SDA) capable of rapidly and dynamically modifying its frequency, radiation, and polarization properties.[63] An SDA provides a marked advantage over a traditional bandwidth or spectrum restricted antennae, in that an SDA can adapt to suit different radio systems, receive multiple input feeds, and provide simultaneous operation of several different radio systems from a single antenna unit. "This in turn could lead to a reduction in the number of installed antennas on a given platform…containing multiple radiating sections."[64] Theoretically, combining multiple phase shifters with appropriately placed SDAs would allow beam steering similar to an active electronically scanned array (AESA) radar antenna.[65] The SDA concept is not new, however as technology around software-defined networks and radios continues to improve, so too will the utility and capabilities of these agile antennas.

Mission Assurance and Cyber Protection

> Given this climate of rapid technological advance and global political change, the USAF recognizes the duality of cyberspace as a war-fighting domain as well as a foundational domain. As a war-fighting domain, cyberspace affords irregular adversaries a low-cost option to attack our global interests. As a foundational domain, cyberspace offers our peers an attack vector to negate our superiority in the traditional domains of land, sea, air, and space.
>
> –Dr. Kamal T. Jabbour, Senior Scientist, Air Force Research Laboratory[66]

In order to succeed in the contested and highly dynamic battlespace of the future, a MMN must not only overcome challenges throughout the EM spectrum, but also threats to the very information it serves to convey. Like any existing terrestrial or wireless network that transfers packets of data through and between multiple nodes, an airborne MMN must sufficiently address threats in the cyber domain. However, unlike a traditional network that functions primarily to move and ensure data, a MMN made up of highly expensive and often unique or numerically limited combat aircraft must not only ensure the integrity of the data within the network, but also that of the nodes themselves. This unique requirement to ensure nodal safety in addition to guaranteeing data integrity makes the "mission assurance" problem even more complicated in an airborne MMN.[67]

Likely the most glaring concern with an "open architecture" (OA) network composed of OMS-compliant systems is its vulnerability to cyber-attack and exploitation. As a result of linking multiple nodes in a single network with a common OMS "language," assets are "arguably more at risk to an asymmetric attack vector launched by an adversary that cannot, or chooses not to, confront the [US forces]" in a conventional manner.[68] In this regard, the nodes of an airborne MMN are similar to the vulnerable satellites in that they are costly to develop and replace, yet vulnerable to threats in a relatively cheap and rapidly adaptable domain. As with any information network, a MMN would be subject to three major types of Information Assurance (IA) threats: *confidentiality* (which may take the form of a hidden advanced persistent threat that affects the confidentiality of the user or node), *destructive attack* (which does not hide, but attacks and degrades information availability), and *access-less attack* (which hijacks traffic to impact integrity of information on the network).[69] Fortunately, the methods for defending information on "traditional" and future software-defined networks have developed hand-in-hand with the conceptual networks themselves.

Dr. Kamal Jabbour (Senior Scientist for Information Assurance in the Air Force Research Laboratory's (AFRL) Information Directorate) suggests that while we "cannot build anything that can never be hacked," there are ways to ensure data integrity for the duration of a specific mission.[70] In a new or future network, such as an airborne MMN, his "Principles of War in the Cyber Domain" offer an alternative approach to developing secure systems, which include "the fundamental [IA] tenets of confidentiality, integrity, availability, authentication, and attribution, as well as state-of-the-practice provision of these tenets through cryptography, diversity, agility, and trust."[71] Under this new mindset, one does not differentiate between "defensive" or "offensive" cyber capabilities, but instead focuses first on the specific mission at hand, then "gray" networks, then threats.[72] An example of prioritizing a specific mission's assurance in this way would be to build a "blank code, a new programing language for that single mission, then delete it after completion."[73] Since time is an important dimension of mission assurance, network engineers could tailor the security requirements for a specific network, to counter threats in a specific geographic region, for a specific time, to ensure data integrity over the duration of a mission.[74]

An additional benefit of a non-linear, non-hierarchical MMN is that IA security policy updates and changes can distribute simultaneously "to the very edges of the network, rather than being confined to a handful of centrally located security devices."[75] This "flat" architecture in a

MMN also benefits encryption key distribution, enabling updates to an entire network in real-time instead of relying on ground crews to update individual platforms independently. However, network users must remain vigilant against multi-dimensional threats to the network, as advanced encryption alone cannot secure a mission. For example, even without the ability to decrypt data, an adversary could disrupt mission effectiveness by targeting a single platform with a corrupting cyber-attack aimed solely at disrupting dataflow through that node. “If packets are going through a node, they can be deleted, spoofed, doubled, or have every-other packet sent…this impacts a mission despite encryption.”[76]

When addressing the threat of cyber vulnerabilities and the science of mission assurance as applied to any network (especially an airborne MMN), we must address an important question of priorities. What is more important: trusting the integrity of information received, or receiving all of the information? Research indicates that integrity and trust supersedes quantity and availability, however the two are so interrelated that one is effectively useless without ensuring the other. New waveforms, encryption keys, processors, sensors, and data types are all equally useless if the integrity of the information they provide cannot be guaranteed. This is why “mission assurance in a contested cyber domain requires a [deliberate] four-step process: (1) *prioritization*, (2) *[mission] mapping,* (3) *vulnerability assessment*, and (4) *threat mitigation*.”[77] Ultimately, the utility of an airborne MMN makes the danger of multi-dimensional asymmetric threats worth the risk. Data distribution is critical to any mission’s success, and combat operations must prioritize and safeguard that information as vigorously as the physical sensors, shooters, and decision makers collecting and ingesting it.

The Art of the Possible: Today and Tomorrow

> The future of warfare in the age of cognition is going to be about networks and data. Does it connect? Good! Can it share? Even better…What would the world look like if we actually connected what we have…if we looked at the world through the lens of a network as opposed to individual platforms? Electronic jamming-shared immediately, avoided automatically. Every 3 minutes a mobility aircraft takes off somewhere on the planet. Platforms? Or nodes in a network?
>
> –Gen David L. Goldfein, Chief of Staff, US Air Force[78]

With the technology available to the USAF today, the survivable, scalable, network of the future does not need to wait until 2035 for operationalization. Both the USAF Future Operating Concept and Air Superiority Flight Plan call for this type of capability, and the "combat cloud" demands it. With those requirements in mind, the USAF could push this capability with JUON-like (Joint Urgent Operational Need) motivation to the field in a fraction of the time required to design and build a new communications satellite. The entire Project Hunter experimentation series, which included LLAN technology, only cost $45.7 million.[79] This sum covered contracts, equipment integration, and multiple ground and airborne demos between dissimilar platforms. When compared to the $500 million price tag of some new satellites (and the additional $300 million to launch them), this technology is cost effective and readily available.[80] In a space denied environment, MMN nodes can include all varieties of aircraft (to include fighters, tankers, mobility assets, airborne C2, etc.), surface and subsurface vessels, and ground sites (both fixed and mobile, such as embedded with a Special Operations Forces [SOF] team). With such variety across potential platforms and nodes across a Joint battlespace, the MMN could even bridge data from the highly contested frontlines back to a ground site with fiber connectivity, to distribute network data anywhere in the world.

An airborne MMN needs more than connectivity to satisfy the needs of the USAF and Joint partners in a high-end fight, and employing this technology on current high-altitude platforms would only be the first step in a much larger system of systems. With modest improvement, the network could provide not only communication and data pathways in a space denied environment, but host processors and mission computers capable of automatically fusing and distributing data over the network. For example, the OMS-compliant Enterprise Mission Computer 2.0 (EMC2), which also flew on the U-2S during Project Hunter experimentation, is capable of integrating "software services, third-party applications, [and] new capabilities quickly without impacting the system architecture of the platform."[81] Such applications could include multi-level security (MLS) enclaves and advanced algorithms to process multi-INT data directly onboard the aircraft. Such processing algorithms could include automatic correlation and fusion of organic and off board SIGINT, followed by automatic tip-and-cue of a networked IMINT sensor either onboard the host aircraft or tasked to a more optimal network node, followed by automatic target recognition (ATR) provided by any of the processor hosts in the MMN. Additional algorithms could distribute the fused intelligence products at any or all stages of this process, to specified nodes via the MMN and other networks as necessary.

OMS connectivity through the airborne MMN could allow automated distribution of this high-fidelity information to selected nodes and/or transmission through an extended network to traditional intelligence or C2 authorities. The ability to share kinetic and non-kinetic targeting solutions at the forward edge of a contested battlespace, especially in an autonomous environment where traditional reachback is impossible, could dramatically enhance and enable the complete kill-chain for advanced multirole assets. Employing this or a like capability on each of the high-altitude nodes could provide disaggregated processing and an environment for machine-to-machine collaboration through advanced algorithms and data sharing.

In addition to covering a capability gap in the event of space degradation or denial, an airborne MMN would satisfy a number of other existing requirements. For example, a survivable network as described would meet or complement each of the four key capability development efforts within the Air Superiority 2030 Flight Plan Enterprise Capability Collaboration Team (ECCT) "Find, Fix, Track, and Assess" segment.[82] These key development efforts include: (1) *Data-to-Decision Campaign of Experiments*, (2) *ISR Collect and Persistent ISR*, (3) *Penetrating Counterair (PCA)*, and (4) *Agile Communications*. The *Data-to-Decision Campaign* seeks to build "the appropriate architectures necessary to integrate and network the…family of capabilities," while *ISR Collect and Persistent ISR* focuses on "multi-domain alternatives for placing the right sensor in the right place at the right time."[83] In a networked approach where "every platform is a sensor," there is greater opportunity to put the appropriate sensor on any given requirement. *Agile Communications* describes almost exactly, the "resiliency and adaptability of integrated networks" with "functionality across multiple platforms, weapons, apertures, and waveforms" that an airborne MMN could provide.[84] Finally, *Penetrating Counterair* would serve as a crucial node of a network, "providing data from its penetrating sensors" and extending the dataflow and C2 capability deep into an enemy's contested or denied battlespace.[85] Overall, these key development efforts seek to gather data from sources across all domains, rapidly analyze and extract operationally relevant information, and distribute the information in the tactically relevant timeline necessary to enable critical decisions and exploit an asymmetric advantage.[86]

The threat of degradation and denial of our space capabilities exists today, justifying the requirement for a rapidly fielded airborne MMN as this research suggests. If prioritized appropriately and implemented as or along the same timeline as a JUON, the USAF could easily pioneer an operational MMN within two years by capitalizing on work already completed and technology currently available.[87] This hypothetical network in 2020 would likely rely heavily on high-altitude ISR platforms, leveraging their increased LOS and mission duration advantages, in addition to readily available SWaP and modularity. As previously mentioned, the adaptable U-2S and RQ-4B can provide an initial software-defined network backbone by hosting the SDR, SDA, and LLAN technology listed above. Project Hunter already demonstrated how quickly and cheaply this technology can enter the operational environment, and should serve as an initial baseline for capabilities on high-altitude nodes. Realistically, the U-2S should employ as a minimum a SDR (likely embedded with the OMS-compliant EMC2), and a compliment of RF antennas (SDAs both omni-directional and directional). The RQ-4B should host a similar set of SDRs, SDAs, and OMS processors, but at a minimum should serve as a relay node with the appropriate antennas.

With such a loadout on the U-2S and RQ-4B fleet, the USAF high-altitude ISR enterprise would be able to demonstrate the benefits of additional data pathways and expanded bandwidth outside of traditional BLOS reachback architectures. With a bit of additional technology, both platforms could really explore the advantages of automated and decentralized processing in the operational environment and serve as gateways (or translators) for dissimilar links and networks in the battlespace. For example, a U-2S serving as an MLS gateway could ingest data from a 5th generation fighter (via Intra-Flight Data Link [IFDL] or Multi-Function Advanced Data Link [MADL]), fuse that data with SIGINT collected organically or brought onboard from a connection to a national asset (if available), and then distribute the final correlated and fused product to any number of potential receivers across any available network or datalink.[88]

The high-altitude platforms in a notional 2020 network serve as central hubs, which host a majority of the network’s processing, MLS enclaves, and translation services. This is not the ideal situation for a MMN, as the failure of one of the central hubs could render the entire network ineffective; however, to expedite fielding, establish a capabilities baseline, and increase inclusivity amongst various platforms, such risks are necessary. Despite deviation from the true nature of a MMN by centralizing much of the processing and employing several different links to be translated in a central hub, high-altitude platforms linked with LLAN would still makeup a proper (though smaller) MMN in the short-term. In a contested environment, these platforms could form a data-bridge from the forward edge of an AOR all the way back to a C2 platform or ground site outside of the adverse effects of jamming or space degradation (see Figure 7). This would still allow the U-2S and RQ-4 to conduct critical ISR missions even without the benefit of high-capacity BLOS connectivity, providing essential data to decision makers in any phase of a conflict. At a minimum, high-altitude platforms would provide a robust LPI/LPD/AJ network with the option to serve as a hub-and-spoke processing or data distribution hubs in a contested environment.[89]

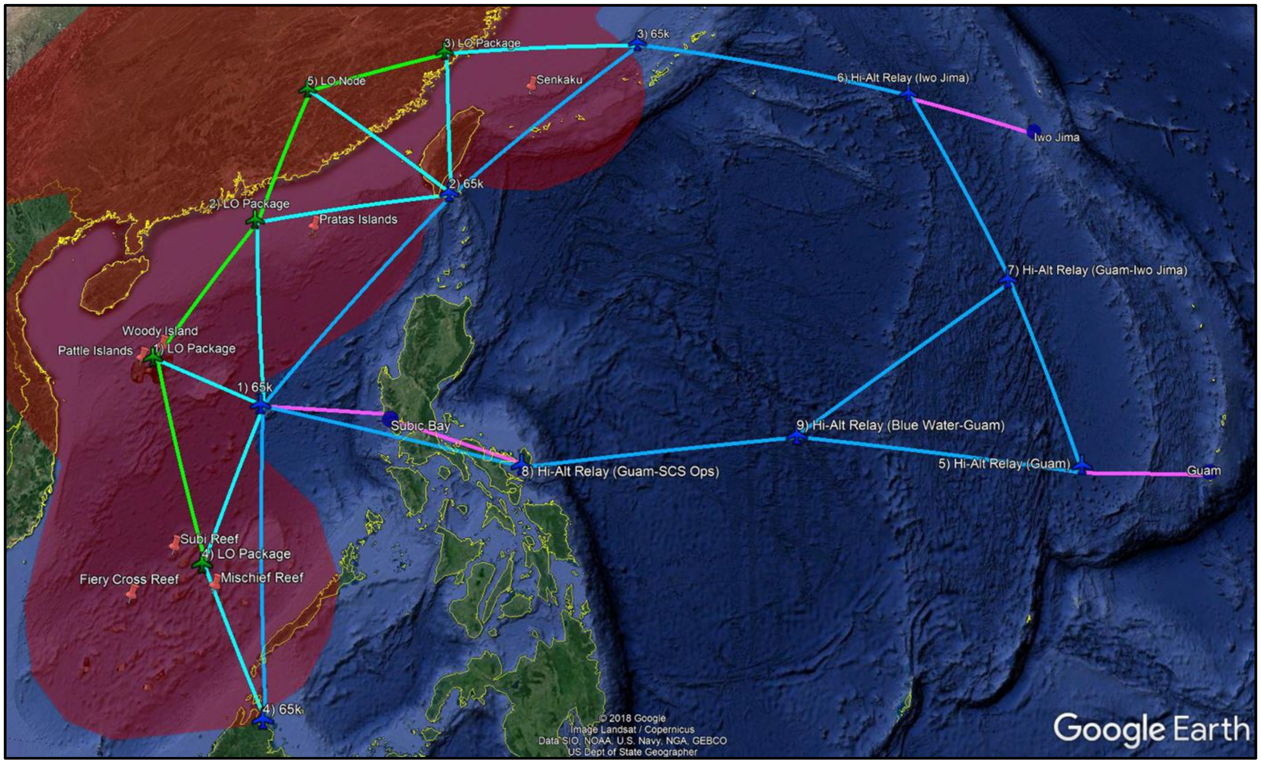


Figure 7 - Example of a High-Altitude "Data Bridge"[90]

Advancing the network into the future by five years opens up several other possibilities for nodes outside of the initial high-altitude ISR platforms. As industry partners are able to produce more SDR and SDA components, other aircraft with available SWaP could receive loadouts similar to the baseline U-2S and RQ-4B, thus increasing the number of nodes and potential data pathways, dramatically improving the resiliency and robustness of the MMN in a given area. If each of the aerial refueling, mobility, and “wide-body” C2 and ISR assets in a given theater were participants of a MMN, the network capabilities and pathways would increase significantly (see Figure 8).[91]

In such a future scenario, as many assets as possible would host some sort of onboard processing capability, thus alleviating the high-altitude platforms of their roles as central hubs, and truly disaggregating the processing power of the network as a whole. This nodal expansion would not be limited to just USAF assets either, but include any aircraft, surface or subsurface vessel, and land component able to host an SDR and antenna. Furthermore, incorporating MMN connectivity onto nodes in a survivable LEO CubeSat constellation (e.g. *Blue Horizons’* ARGOS), could extend the network’s connectivity to a global scale. The benefits of such an expansion for “blue force” tracking, as well as common operating picture (COP) distribution and internet protocol (IP) dataflow to and from networked assets goes without saying.

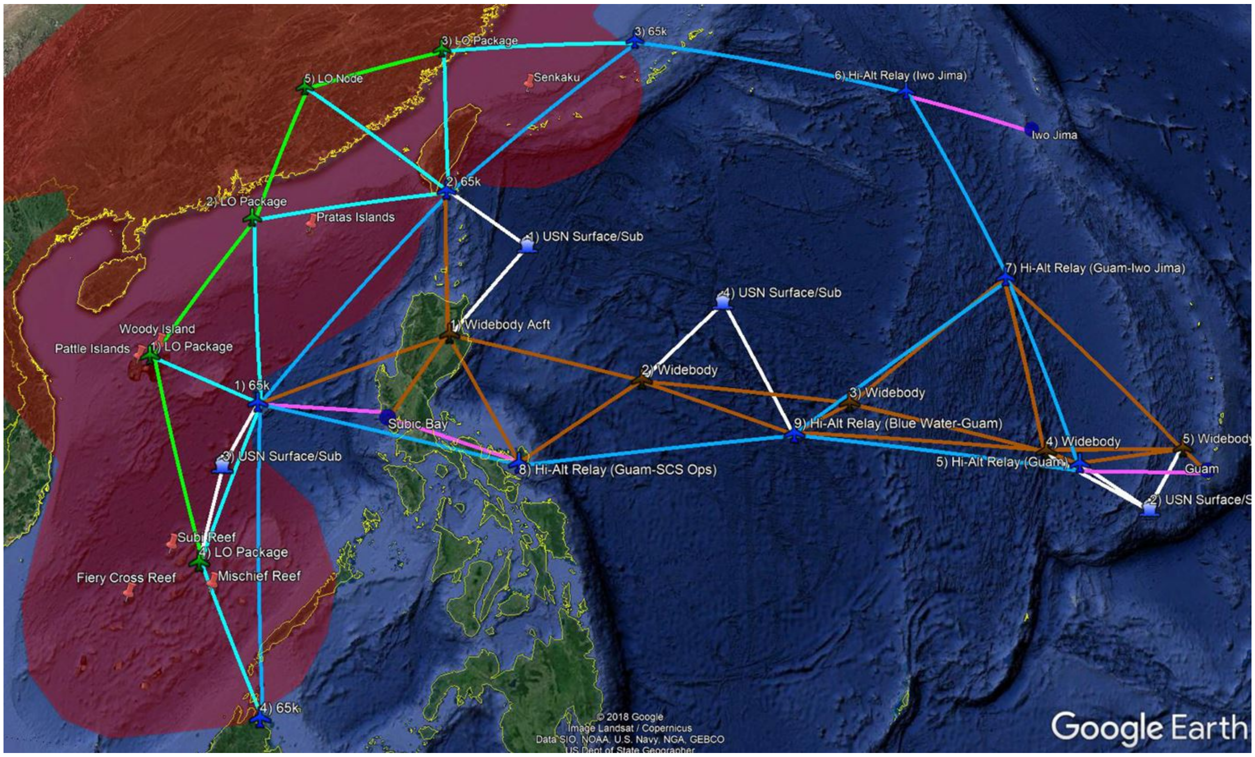


Figure 8 - Example Network in 5 Years[92]

While expanding the MMN infrastructure to as many assets as possible, there still would likely be challenges in incorporating either a new internal SDR or external antennas onto LO platforms. This is because it is inherently difficult and commensurately expensive to alter LO surfaces, making additional conformal or non-conformal antennas difficult. That is not to say that a new SDA on an existing 5th generation platform is impossible, just far more expensive than other platforms. For new assets such as the B-21 that already require OMS compatibility, it may be possible to incorporate an appropriate array of SDAs onto the platform still in development (if such a requirement is not already included). Ultimately, MMN inclusion should be as un-intrusive to the forward-edge assets as possible, suggesting that a different asset should again act as a translator, relay, and processor to circumvent the high cost of 5th generation alterations. Once again, the modular high-altitude platforms provide a comparatively low-cost option to integrate the immense benefits of 5th generation data into a MMN, while providing the necessary MLS enclaves to incorporate and properly distribute the highly classified data they produce.

If an SDR or new antenna were impossible due to cost or physics limitations on a 5th generation asset, the benefits of AESA radars may help bridge the gap. It is not feasible to add an antenna to a 5th generation aircraft's skin without either incurring high cost or degrading the platform's LO characteristics. However, a small hardware addition inside the airframe combined with an appropriate software upgrade for user-interface could allow an operator to toggle a radar between "normal" fighter functions and new wideband communication modes.[93] Naturally another platform would be required to receive the wideband data from the LO asset and either process it or relay to a different node in the MMN for correlation, fusion, or relay as necessary. In this theoretical five-year future network, a U-2S wielding an ASARS-2C AESA radar and appropriate processors could serve as the receiving asset in an X-band-to-X-band data exchange. Additionally, an RQ-4 Block 40 employing a ZPY-2 AESA and associated processors may be able to receive 5th generation wideband information.[94]

By the 10-year mark, a theater-wide MMN should connect the entire Joint Force, from aircraft to SOF teams, and surface terminals to satellites. In this future scenario, several assets to include ISR and wide-body platforms should host a number of algorithms to enable net-centric geolocation, automated correlation and fusion of any OMS sensor node, algorithms to ensure appropriate MLS data distribution, all enhanced by real-time machine learning within the network. This would be an example of an "intelligent radio" on a grand scale. At some point prior to a 10-year mark, several weapons would also become nodes in the MMN, benefiting from the real-time intelligence and targetable coordinates on the network while enroute to their projected targets.[95]

An additional benefit to a disseminated MMN is its ability to offer PNT synchronization services as an alternative to GPS, providing some diversity in PNT sources within an A2AD environment.[96] In such a scenario, an asset with an alternative means of navigation and a precise timing clock could provide location data to other users within the network and mitigate or negate the loss of a GPS signal. For example, a high-altitude aircraft such as a U-2S with a celestial object sighting system (COSS) and a precise clock (such as a high-performance Rubidium Oscillator) could determine its location by tracking stars and satellites, regardless of GPS jamming or inclement weather.[97] The host platform could then disseminate a PNT solution to other nodes, facilitating navigation and synchronization at varying qualities across the network. As is true with most functions of a MMN, the more nodes providing data (in this case organic PNT derived from non-GPS sources), the higher the quality and resilience of the network as a whole. Just as more GPS satellites in view produce a higher fidelity position, so too would more COSS nodes in a MMN providing PNT throughout the whole network.

Recommendations

> We have no God-given right to victory on the battlefield, and in that regard make no mistake that our adversaries are right now making concentrated efforts to erode our competitive edge… if you look at outer space which was long considered a sanctuary of sorts, it's now contested…So if we fail to adapt at the speed of relevance, then our forces, military forces, our Air Force, will lose the very technical and tactical advantages we've enjoyed since World War II…Because the paradox of war is the adversary will always move against your perceived weakness.
>
> –Hon. James N. Mattis, Secretary of Defense[98]

Air Superiority 2030 highlights that "[t]he speed of capability development and fielding will be critical to retain the U.S. advantage in the air. As the pace of technological advancements continue [sic] to increase, the Air Force must leverage experimentation and prototyping to more rapidly infuse advanced technologies into the force."[99] Considering the technology already exists, has succeeded in robust testing and experimentation, and answers numerous existing and future requirements, the USAF should prioritize immediate LLAN operationalization within the high-altitude fleet of ISR aircraft. This initial fielding will enable the small but agile high-altitude ISR fleet to begin developing tactics, techniques, and procedures (TTPs) for airborne MMN employment in the operational environment. Aircrew, intelligence analysts, and C2 entities must begin familiarizing with adaptive networks that can grow much larger than any current airborne network in the operational environment. Data sharing between dissimilar platforms (initially high altitude platforms like U-2S and RQ-4B) in different environments, at different ranges, and with different data rates will help shape future expectations and bandwidth management when the network expands to additional platforms (ISR, fighter, bomber, mobility, etc.).

A roadmap for the LLAN enabled airborne MMN in the near future should begin with identifying an appropriate agency for program accountability. This authority would be responsible for coordinating acquisition priorities, to include: (1) Programming modernization funds for the multi-platform network; (2) Coordinating with necessary organizations (probably A2/A3/AQ/AFMC) to agree on specific standards, interfaces, etc., for the multi-platform network and formally commit to them; (3) Ensuring individual requirements shops prioritize the requirement. With standards and requirements formalized, the actual hardware should aim to enter the operational environment within 24 months to meet JUON timelines.

This initial fielding would occur within the high-altitude fleet, but expand as rapidly as possible to other platforms capable of hosting an SDR, processor, or appropriate relay antenna. Once the ISR enterprise demonstrates the power of a stable, standardized, advanced MMN, other platforms should employ the necessary hardware, antennas, and interfaces as quickly as possible. The priority for a “second wave” of MMN nodes should be on network inclusion, not necessarily hardware and software implementation. That is to say, connecting 5th generation platforms and including the exquisite data that they provide just by virtue of operating in the battlespace (via dedicated reconnaissance tasking or via “non-traditional ISR) would be a priority. Since it is expensive and difficult to make alterations to LO surfaces however, rapid network inclusion may require some nodes to serve initially as “translators” and MLS gateways. Including 5th generation and LO assets will extend the network coverage into contested and denied airspace, enabling data to flow between forward edge assets in a fight, through ISR platforms with extreme LOS advantages and onboard processors, to C2 and decision makers in the AOR.

Once the high-altitude fleet and LO platforms are connected, additional platforms of all types should receive at least minimum hardware and software requirements to function as connective nodes. This would include tanker aircraft, battle management, command and control (BMC2) platforms, air mobility, and 4th generation fighters and bombers to increase network size and reach, with the hope of always maintaining connectivity from the denied environment out to a non-contested area. Ultimately, this network would evolve from a rapidly available coverage of a potential capability gap, to the standard network for the entire Joint force, turning every connected platform into a sensor (see Figure 9).

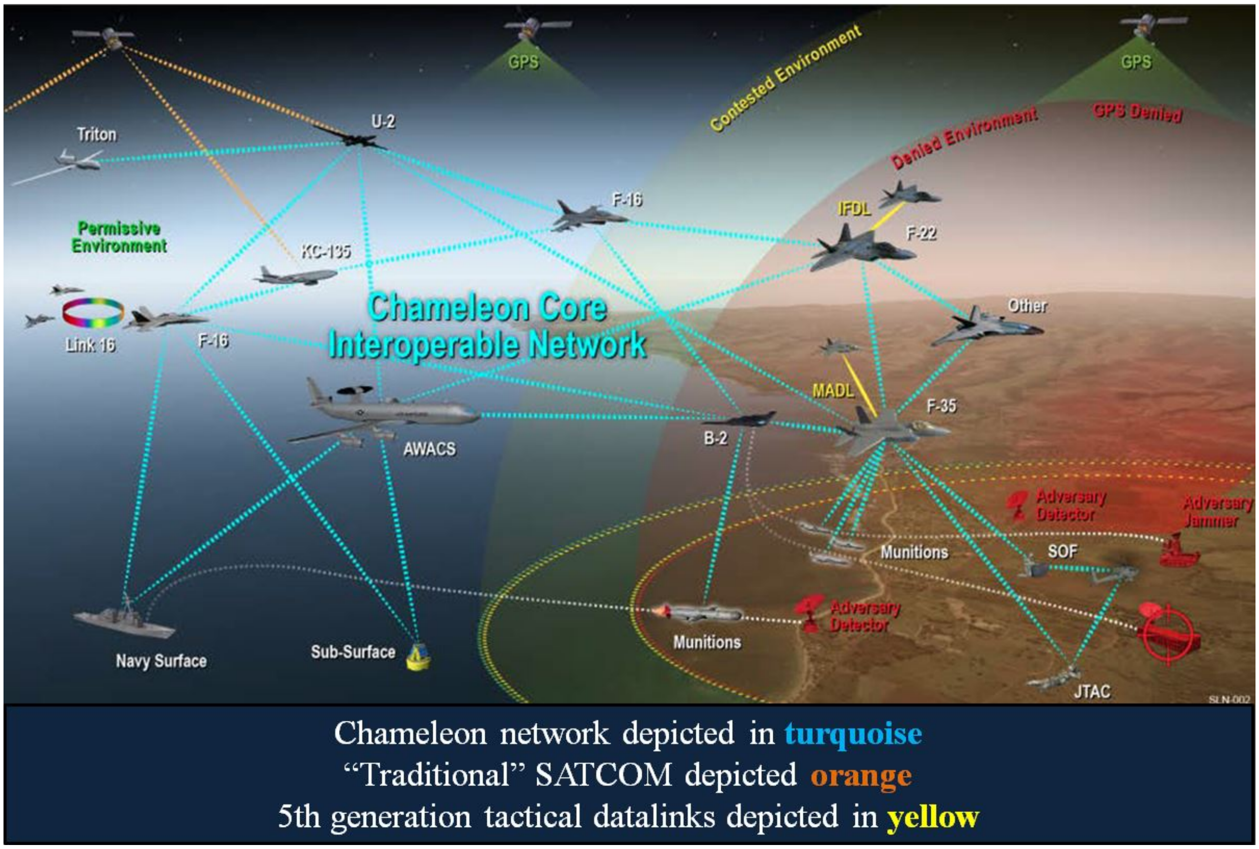


Figure 9 - Example Future Network Using Chameleon[100]

Conclusion

> You can be sure of succeeding in your attacks if you only attack places which are undefended...The spot where we intend to fight must not be made known…So in war, the way is to avoid what is strong and to strike at what is weak.
>
> –Sun Tzu[101]

The USAF is at a position of extreme disadvantage when facing the vast array of capable threats to its space assets. As Clausewitz teaches, employing a preponderance of forces at a decisive point is a necessary principle for victory.[102] In our case, an adversary's relatively cheap and numerically superior arsenal of ASAT capabilities against an undefended, exceptionally expensive and critical network of satellites is a recipe for battlefield disaster. Space is no longer a sanctuary, and our satellite systems "lose the cost-exchange battle" with enemy ASATs, DE weapons, and both dumb and cognitive jammers.[103] The USAF and Joint partners regularly rely on the services that space assets provide, and in their absence, would fight at tremendous disadvantage. Fortunately, forward thinking planners, engineers, and tacticians developed some of the technological tools necessary to overcome some of our modern vulnerability, well in advance of the Future Operating Concept's timeline. What remains is actual operational implementation of the airborne MMN, first on high-altitude ISR platforms, and then throughout the rest of the USAF and Joint force. A fully capable layer of fully networked and survivable nodes in the air domain can mitigate many of the threats to our space infrastructure. The technology is already here, we just need to properly prioritize its fielding in response to existing threats, capability gaps, and future requirements. It is time to get connected, so that we can start sharing, and start learning.

NOTES

[1] Hon. Heather A. Wilson, Secretary of the Air Force (address, Air Force Association Air, Space & Cyber Conference, National Harbor, MD, 18 September 2017), https://www.afa.org/airspacecyber/conference2017/recordings.

[2] Hon. James N. Mattis, Secretary of Defense (address, Air Force Association Air, Space & Cyber Conference, National Harbor, MD, 20 September 2017), https://www.afa.org/airspacecyber/conference2017/recordings.

[3] Gen David L. Goldfein, chief of staff, US Air Force (address, Air Force Association Air, Space & Cyber Conference, National Harbor, MD, 19 September 2017), https://www.afa.org/airspacecyber/conference2017/recordings.

[4] Brian Weeden and Victoria Samson, *Global Counterspace Capabilities: An Open Source Assessment* (Washington, DC: Secure World Foundation, 2018), 10.

[5] The five categories of counterspace capabilities are: direct-ascent, co-orbital, electronic warfare, directed energy, and cyber. Ibid.

[6] While Link-16 is normally exchanged across and through radio frequencies, the network can also be exchanged over landline and satellite links. It operates at UHF frequencies and therefore direct communications are only possible when the transmitter and receiver are in line-of-sight. Thales UK, *Link 16 Operational Overview*, Thales Group white paper (Somerset, UK: Horizon House), 2,

[7] Steven M. Kosiak, *Arming the Heavens: A Preliminary Assessment of the Potential Cost and Cost-Effectiveness of Space-Based Weapons* (Washington, DC: Center for Strategic and Budgetary Assessments, 2007), *ii*.

[8] Marcus Weisgerber, "US Air Force Is Moving Faster on Space Contracts, Industry Execs Say," *Defense One*, 17 April 2018, https://www.defenseone.com/business/2018/04/air-force-faster-satellite-contracts-industry/147531/?oref=d-river&utm_source=Sailthru&utm_medium=email&utm_campaign=EBB%204.18.18&utm_term=Editorial%20-%20Military%20-%20Early%20Bird%20Brief.

[9] Valerie Insinna, "Air Force Sets Ambitious Goal to Procure Next Missile Warning Satellites in Five Years," *Defense News*, 17 April 2018, https://www.defensenews.com/digital-show-dailies/space-symposium/2018/04/18/air-force-sets-ambitious-goal-to-procure-next-missile-warning-satellites-in-five-years/?utm_source=Sailthru&utm_medium=email&utm_campaign=EBB%204.18.18&utm_term=Editorial%20-%20Military%20-%20Early%20Bird%20Brief.

[10] Aircraft capable of sustained operations at and above 55,000 feet MSL are considered "high-altitude" platforms. Within the US Air Force such platforms include the U-2S and variants of RQ-4B. Additionally, NASA's WB-57 is also capable of high-altitude operations.

[11] Gen John W. Raymond, Commander, Air Force Space Command (address, Air Force Association Air, Space & Cyber Conference, National Harbor, MD, 19 September 2017), https://www.afa.org/airspacecyber/ conference2017/recordings.https://www.afa.org/airspacecyber/conference2017/recordings.

[12] United States Air Force. *Air Force Future Operating Concept: A View of the Air Force in 2035,* Sep 2015, 9, http://www.af.mil/Portals/1/images/airpower/AFFOC.pdf.

[13] Ibid., 19.

[14] Colin Clark, "Chinese ASAT Test Was 'Successful:' Lt. Gen. Raymond," *Breaking Defense*, 14 Apr 2015, https://breakingdefense.com/2015/04/chinese-asat-test-was-successful-lt-gen-raymond/.

[15] House, *China's Progress with Directed Energy Weapons: Testimony before the U.S.-China Economic and Security Review Commission hearing, "China's Advanced Weapons,"* Washington, D.C., 23, Feb 2017, https://www.uscc.gov/sites/default/files/Fisher_Combined.pdf.

[16] Weeden, *Global Counterspace*, 20.

[17] Ashton B. Carter, "The Relationship of ASAT and BMD Systems," *Daedalus*, 114, no. 2, 1985, 171-189, http://www.jstor.org/stable/20024984.

[18] United States Air Force, *Future Operating Concept*, 9.

[19] Weeden, *Global Counterspace*, 65-68.

[20] James Black, "Our Reliance on Space Tech Means We Should Prepare for the Worst," *Defense News, 12 March 2018,* https://www.defensenews.com/space/2018/03/12/our-reliance-on-space-tech-means-we-should-prepare-for-the-worst/.

[21] Ibid.

[22] Jessica Orwig, "The Amount of Space Junk Around Earth Has Hit a 'Critical Density'–And It Could Jeopardize Our Space Missions," *Business Insider*, 23 September 2015, http://www.businessinsider.com/space-junk-at-critical-density-2015-9.

[23] NASA defines SmallSats as spacecraft with a mass less than 180 kilograms, about the size of a refrigerator. CubeSats are a class of "nanosatellites" that use a standard size and form factor (1-10 kilograms). These satellites can operate independently or in mini-constellations or "swarms" to provide services similar to the larger and more expensive systems. For example, a disaggregated constellation of small SAR collectors could theoretically generate products at a quality equal or exceeding existing collectors. Elizabeth Mabrouk, "What Are SmallSats and CubeSats?" *NASA*, 7 August 2017, https://www.nasa.gov/content/what-are-smallsats-and-cubesats.

[24] Judy Corbett, "Micrometeoroids and Orbital Debris (MMOD)," *NASA*, 6 August 2017, https://www.nasa.gov/centers/wstf/site_tour/remote_hypervelocity_test_laboratory/micrometeoroid_and_orbital_debris.html.

[25] Mr. Bryan Lima, Program Director for Manned C2 ISR, Northrop Grumman Aerospace Systems (address, Air Force Association Air, Space & Cyber Conference, National Harbor, MD, 18 September 2017), https://www.afa.org/airspacecyber/conference2017/recordings.

[26] Primavera De Filippi, "It's Time to Take Mesh Networks Seriously (And Not Just For the Reasons You Think)," *Wired*, 2 January 2014, https://www.wired.com/2014/01/its-time-to-take-mesh-networks-seriously-and-not-just-for-the-reasons-you-think/.

[27] John Edwards, *Rethinking ISR: How Innovations Like SDN Change the ISR Mission*, C4ISR & Networks editorial white paper, (Sightline Media Group), 2, www.C4ISRNET.com/wp/RedefineISR.

[28] Archive image from DailyWireless.org. Custom overlays added by author. Accessed 1 May 2018, http://www.dailywireless.org/2005/01/06/wireless-recon-airplanes/

[29] *Wikipedia*, s.v. "Mesh Networking ," accessed 5April 2018, https://en.wikipedia.org/wiki/Mesh_networking

[30] De Filippi, "Mesh Networks," https://www.wired.com/2014/01/its-time-to-take-mesh-networks-seriously-and-not-just-for-the-reasons-you-think/.

[31] Morteza M. Zanjireh and Hai Larijani, *A Survey on Centralised and Distributed Clustering Routing Algorithms for WSNs*, conference paper (Glasgow, UK: School of Engineering and Built Environment, 2015), 2.

[32] See Morteza for specific detail and examples of routing protocol, scalability, and various network types.

[33] For the sake of this research, MMN and MANET are shall be used interchangeably.

[34] Airborne Wireless Network, "Airborne Wireless Network Wholesale Carrier Network," accessed 24 February 2018, http://www.airbornewirelessnetwork.com.

[35] Ibid.

[36] Ibid.

[37] Lt Gen Charles R. Davis, USAF (Ret.), Senior Vice President for Strategic Development, L3 Technologies (address, Air Force Association Air, Space & Cyber Conference, National Harbor, MD, 18 September 2017), https://www.afa.org/airspacecyber/conference2017/recordings.

38. Air Force Research Laboratory. ISR Science & Technology Strategy, 11 Jun 2011, www.defenseinnovationmarketplace.mil/.../AFRL-ISR_FINAL-PA-APPRVD.pdf.

39. Rutrell Yasin, *Next-Generation Communications: What Network Services 2020 and Global Network Services Will Mean for You*, C4ISR & Networks editorial white paper, (Sightline Media Group), 2, www.C4ISRNET.com/wp/NextGenTelecom.

40. Lt Gen David A. Deptula, USAF (Ret.), "Evolving Technologies and Warfare in the 21st Century: Introducing the 'Combat Cloud,'" *Mitchell Institute Policy Papers*, Vol. 4, Sep 2016, 1, http://docs.wixstatic.com/ugd/a2dd91_73faf7274e9c4e4ca605004dc6628a88.pdf.

41. Ibid.

42. Edwards, *Rethinking ISR*, 2.

43. Lt Gen VeraLinn Jamieson, Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance, Headquarters US Air Force, (address, Air Force Association Air, Space & Cyber Conference, National Harbor, MD, 18 September 2017), https://www.afa.org/airspacecyber/conference2017/recordings.

44. True LOS equation: $R_{NM} = 1.06\left(\sqrt{h_{radar}} + \sqrt{h_{target}}\right) \, with \, h \, in \, ft.$

45. Air Force Fact Sheet, *RQ-4 Global Hawk*, 27 Nov 2014, http://www.af.mil/About-Us/Fact-Sheets/Display/Article/104516/rq-4-global-hawk/.

46. Air Force Fact Sheet, *U-2S/TU-2S*, 23 Nov 2015, http://www.af.mil/About-Us/Fact-Sheets/Display/Article/104560/u-2stu-2s/.

47. This scenario is dependent on geographical location, satellite relay type, and adversary ASAT capabilities. If the adversary launched a kinetic weapon against a specific constellation of satellites, the example is not applicable, however if the adversary is employing barrage or directed jamming against "local" satellites, the high-altitude platforms could reach beyond the physical limits of the jammer.

48. Staff Sgt. Jeffrey Schultze, 9th Reconnaissance Wing Public Affairs, "U-2 makes first appearance during Northern Edge 17," *Pacific Air Forces News*, 19 May 2017, http://www.pacaf.af.mil/News/Article-Display/Article/1187347/u-2-makes-first-appearance-during-northern-edge-17/.

49. Marisa Alia-Novobilski, Air Force Research Laboratory, "AFRL's AgilePod Shows ISR Versatility During Scorpion Fit Test," *Wright-Patterson Air Force Base News*, 2 January 2018, http://www.wpafb.af.mil/News/Article-Display/Article/1406999/afrls-agilepod-shows-isr-versatility-during-scorpion-fit-test/.

50. Note: Illustration serves only to demonstrate basic LOS concepts and is not drawn to scale. The type, position, elevation, and power output of the jammer, as well as satellite relay orbit positions, and high-altitude platform's position relative to the jammer and satellites could all change the scenario. Satellite, U-2, Earth, and Dish are all ClipArt images from Microsoft PowerPoint 2010.

51. LPD/LPI/AJ (LLAN) Program, "Final Report," 2 October 2017, 1.

52. Ibid.

53. Ibid., 2.

54. A summary of LLAN attributes from the "LLAN Final Report" is available in the "UNCLASSIFIED//FOR OFFICIAL USE ONLY" version of this research.

55. Ibid., 97.

56. Eugene Grayver, *Implementing Software Defined Radio* (New York, NY: Springer, 2013), 5.

57. "What is ALE?" HF Link, http://hflink.com/automaticlinkestablishment/.

58. "What is Software Defined Radio?" Wireless Innovation Forum, 2017, https://www.wirelessinnovation.org/Introduction_to_SDR.

59. Ibid.

60. Ibid.

61. Robert Edilson, "Rockwell Collins Demonstrates new Directional Communication Link with Longer Range and Anti-Jamming Capability," *Rockwell Collins*, 14 September 2017, https://www.rockwellcollins.com/Data/News/2017-Cal-Yr/GS/20170914-ATC-Directional-Comms.aspx.

62. Ibid.

63. Jennifer T. Bernhard, "Reconfigurable Antennas," *Synthesis Lecture on Antennas*, Vol. 2, No. 1, 2007, 1, https://www.morganclaypool.com/doi/abs/10.2200/ S00067ED1V01Y200707ANT004

64. S. P. Benham, D. P. Atkins, E. J. Totten, G. A. Pettitt and P. Cushnaghan, "Software defined antenna," *2009 Loughborough Antennas & Propagation Conference*, Loughborough, 2009, 489.

[65] Tamara Wilhite, “An Introduction to Software Defined Antennas,” *TurboFuture*, 8 January 2018, https://turbofuture.com/industrial/An-Introduction-to-Software-Defined-Antennas.

[66] Dr. Kamal Jabbour, “Cyber Vision and Cyber Force Development,” *Strategic Studies Quarterly*, Spring 2010, 64, http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-04_Issue-1/Jabbour.pdf.

[67] DoDD 3020.40 defines Mission Assurance “as a process to protect or ensure the continued function and resilience of capabilities and assets by refining, integrating, and synchronizing the aspects of the DoD security, protection, and risk-management programs that directly relate to mission execution.” Department of Defense DoD Directive 3020.40, *Mission Assurance*, 29 November 2016, 3, http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040_dodd_2016.pdf.

[68] Dr. Kamal Jabbour and Sarah Muccio, “The Science of Mission Assurance,” *Journal of Strategic Security*, Vol. 4, No. 2, Summer 2011, 61.

[69] Dr. Kamal Jabbour, “The Information High Ground: Cyber War” (lecture, Air Command & Staff College, Maxwell AFB, AL, 8 February 2018.

[70] Ibid.

[71] Jabbour, *Mission Assurance*, 63.

[72] Jabbour, “Information High Ground,” lecture.

[73] Ibid.

[74] Jabbour, *Mission Assurance*, 72.

[75] Adam Stone, *Embracing Software-Defined Networking: How to Overcome 4 Critical Management Challenges in Virtual Networks*, C4ISR & Networks editorial white paper, (Sightline Media Group), 4, www.C4ISRNET.com/wp/virtualnetworks.

[76] Jabbour, “Information High Ground,” lecture.

[77] Jabbour, *Mission Assurance*, 67.

[78] Goldfein, address, 19 September 2017.

[79] Capt Mary Nelson, AFLCMC/HNJ, “Project Hunter Speaker Series,” (briefing, digital slides, 22 August 2017).

[80] The recent loss of the classified ZUMA payload atop a Falcon 9 only makes this point more important. Space launch is not a guarantee even with modern capabilities. Dana Hull Sonali

Basak, "Taxpayers May Pay for Secret ZUMA Satellite Lost After SpaceX Launch," 18 January 2018, http://www.latimes.com/business/la-fi-spacex-zuma-cost-20180118-story.html.

81. Katherine Owens, "Lockheed enterprise computer connects older aircraft with F-35s," *Defense Systems*, 7 Jun 2017, https://defensesystems.com/articles/2017/06/08/lockheed-drone.aspx.

82. United States Air Force, *Air Superiority 2030 Flight Plan: Enterprise Capability Collaboration Team*, May 2015, www.af.mil/Portals/1/.../airpower/Air%20Superiority%202030%20Flight%20Plan.pdf.

83. Ibid.

84. Ibid.

85. Ibid.

86. Ibid.

87. Department of Defense, *Report of the Defense Science Board Task Force on the Fulfillment of Urgent Operational Needs*, July 2009 (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics), 4.

88. It is worth noting that the Project Hunter experiments at NORTHERN EDGE in 2017 actually employed these capabilities. The aircraft hosted an IFDL/MADL radio, a Link-16 radio, and the correlation and fusion engine which would be present on the EMC2 (though this fusion engine did not actually exist on the aircraft due to timing constraints at the time, so the data had to move from the aircraft through the traditional BLOS link architecture for processing at a ground site, then return to the aircraft for Link-16 dissemination).

89. Julie Miller, Lockheed Martin, "Synergistic Full Spectrum Operations," (briefing, digital slides, 25 January 2018).

90. Image created by author using Google Earth Pro tools and overlays. Google Earth Pro V 7.3.1.4507. (13 December 2015). Western Pacific. 15° 36.585' N, 129° 21.329' E, Eye alt 1869.30 mi. US Dept of State Geographer, Landsat/Copernicus, NOAA, US Navy, NGA, GEBCO.

91. Examples include: C-17, C-5, C-130, KC-10, KC-135, KC-46, E-2, E-3, E-8, and any other aircraft with space available (such as the MQ-25, or MQ-9 follow-on). These aircraft are more numerous than the U-2S and RQ-4B in, and are common in any AOR. It is not unreasonable to assume that a C-17 (or other wide-body aircraft) has internal rack space for a small SDR and a spot on the airframe for a number of antennas.

92. Google Earth Pro, Western Pacific.

[93] Sean Gallagher, "Radars Perform Double Duty as High-Speed Data Links," *Defense Systems*, 2 July 2009, https://defensesystems.com/articles/2009/07/08/defense-it1-radar.aspx.

[94] This exchange would optimally occur in the X-band between an ASARS-2C or modified ZPY-2 and an APG-81. The assumption being that a 4-ship of F-35 would operate within an A2AD "bubble" and communicate via MADL in an LPI/LPD mode, thus unable to pass any data outside of the immediate flight. In such a scenario, it is likely that at a given time, two of the aircraft would be facing away from the target threat and back toward "blue" forces, enabling acquisition of the U-2S or RQ-4 Blk 40 at range, and a momentary data-burst to the high-altitude receiver. Simultaneously, the U-2S or RQ-4 Blk 40 (which is not LO nor worried about employing an active sensor) could pass critical data directly to the F-35 via a large X-band transmission with little danger of revealing the LO assets' location).

[95] LLAN experimentation at NORTHERN EDGE has already included the AGM-158 family of weapons (specifically LRASM) in a MMN. In the experimentation, an LRASM surrogate received updated target-track data from an FMV asset and a U-2 via the Chameleon waveform and made appropriate adjustments while inflight to the target area, all in a heavily contested EM environment.

[96] LLAN, "Final Report," 2.

[97] Microsemi, "Portfolio of High-Performance Rubidium Oscillators," 2014, https://defensesystems.com/articles/2009/07/08/defense-it1-radar.aspx.

[98] Mattis, address, 20 September 2017.

[99] Air Force, *Air Superiority 2030*.

[100] LLAN, "Final Report," 2.

[101] Sun Tzu, *The Art of War*, trans. Lionel Giles (Blacksburg, VA: Thrifty Books, 2009), 6-7, 16, 30.

[102] Carl von Clausewitz, *On War*, ed. And trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 566.

[103] Miller, "Synergistic Operations," briefing.

BIBLIOGRAPHY

Airborne Wireless Network. “Airborne Wireless Network Wholesale Carrier Network,” accessed 24 February 2018. http://www.airbornewirelessnetwork.com.

Air Force Fact Sheet. *RQ-4 Global Hawk*. 27 Nov 2014. http://www.af.mil/About-Us/Fact-Sheets/Display/Article/104516/rq-4-global-hawk/.

——. *U-2S/TU-2S*. 23 Nov 2015. http://www.af.mil/About-Us/Fact Sheets/Display/Article/104560/u-2stu-2s/.

Air Force Research Laboratory. ISR Science & Technology Strategy, 11 Jun 2011. www.defenseinnovationmarketplace.mil/.../AFRL-ISR_FINAL-PA-APPRVD.pdf.

Alia-Novobilski, Marisa, Air Force Research Laboratory. “AFRL’s AgilePod Shows ISR Versatility During Scorpion Fit Test.” *Wright-Patterson Air Force Base News*, 2 January 2018. http://www.wpafb.af.mil/News/Article-Display/Article/1406999/afrls-agilepod-shows-isr-versatility-during-scorpion-fit-test/.

Basak, Dana Hull Sonali. “Taxpayers May Pay for Secret ZUMA Satellite Lost After SpaceX Launch,” 18 January 2018. http://www.latimes.com/business/la-fi-spacex-zuma-cost-20180118-story.html.

Benham, S. P., D. P. Atkins, E. J. Totten, G. A. Pettitt and P. Cushnaghan. "Software defined antenna." *2009 Loughborough Antennas & Propagation Conference*. Loughborough, 2009.

Bernhard, Jennifer T. “Reconfigurable Antennas.” *Synthesis Lecture on Antennas*, Vol. 2, No. 1, 2007.https://www.morganclaypool.com/doi/abs/10.2200/S00067ED1V01Y200707ANT004

Black, James. “Our Reliance on Space Tech Means We Should Prepare for the Worst,” *Defense News, 12 March 2018.* https://www.defensenews.com/space/2018/03/12/our-reliance-on-space-tech-means-we-should-prepare-for-the-worst/.

Carter, Ashton B. “The Relationship of ASAT and BMD Systems,” *Daedalus*, 114, no. 2, 1985. http://www.jstor.org/stable/20024984.

Clark, Colin. “Chinese ASAT Test Was ‘Successful:’ Lt. Gen. Raymond,” *Breaking Defense*, 14 Apr 2015. https://breakingdefense.com/2015/04/chinese-asat-test-was-successful-lt-gen-raymond/.

Clausewitz, Carl von. *On War*. Edited and translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1976.

Corbett, Judy. "Micrometeoroids and Orbital Debris (MMOD)," *NASA*, 6 August 2017. https://www.nasa.gov/centers/wstf/site_tour/remote_hypervelocity_test_laboratory/micrometeoroid_and_orbital_debris.html.

Davis, Lt Gen Charles R., USAF (Ret.), Senior Vice President for Strategic Development, L3 Technologies. Address. Air Force Association Air, Space & Cyber Conference, National Harbor, MD, 18 September 2017.

De Filippi, Primavera. "It's Time to Take Mesh Networks Seriously (And Not Just For the Reasons You Think)," *Wired*, 2 January 2014. https://www.wired.com/2014/01/its-time-to-take-mesh-networks-seriously-and-not-just-for-the-reasons-you-think/.

Department of Defense (DOD) Directive 3020.40. *Mission Assurance*, 29 November 2016. http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040_dodd_2016.pdf.

Department of Defense. *Report of the Defense Science Board Task Force on the Fulfillment of Urgent Operational Needs*. Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. July 2009.

Deptula, Lt Gen David A. Deptula, USAF (Ret.). "Evolving Technologies and Warfare in the 21st Century: Introducing the 'Combat Cloud.'" *Mitchell Institute Policy Papers*, Vol. 4, Sep 2016. http://docs.wixstatic.com/ugd/a2dd91_73faf7274e9c4e4ca605004dc6628a88.pdf.

Edilson, Robert. "Rockwell Collins Demonstrates new Directional Communication Link with Longer Range and Anti-Jamming Capability." *Rockwell Collins*, 14 September 2017. https://www.rockwellcollins.com/Data/News/2017-Cal-Yr/GS/20170914-ATC-Directional-Comms.aspx.

Edwards, John. *Rethinking ISR: How Innovations Like SDN Change the ISR Mission*. C4ISR & Networks editorial white paper. www.C4ISRNET.com/wp/RedefineISR.

Gallagher, Sean. "Radars Perform Double Duty as High-Speed Data Links." *Defense Systems*, 2 July 2009. https://defensesystems.com/articles/2009/07/08/defense-it1-radar.aspx.

Goldfein, Gen David L., chief of staff, US Air Force. Address. Air Force Association Air, Space & Cyber Conference, National Harbor, MD, 19 September 2017.

Grayver, Eugene. *Implementing Software Defined Radio*. New York, NY: Springer, 2013.

HF Link. "What is ALE?" http://hflink.com/automaticlinkestablishment/.

House. *China's Progress with Directed Energy Weapons: Testimony before the U.S.-China Economic and Security Review Commission hearing, "China's Advanced Weapons,"* Washington, DC, 23, Feb 2017. https://www.uscc.gov/sites/default/files/Fisher_Combined.pdf.

Insinna, Valerie. “Air Force Sets Ambitious Goal to Procure Next Missile Warning Satellites in Five Years,” *Defense News*, 17 April 2018. https://www.defensenews.com/digital-show-dailies/space-symposium/2018/04/18/air-force-sets-ambitious-goal-to-procure-next-missile-warning-satellites-in-five-years/?utm_source=Sailthru&utm_medium=email&utm_campaign=EBB%204.18.18&utm_term=Editorial%20-%20Military%20-%20Early%20Bird%20Brief.

Jabbour, Kamal, Ph.D. “Cyber Vision and Cyber Force Development.” *Strategic Studies Quarterly*, Spring 2010. http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-04_Issue-1/Jabbour.pdf.

——. “The Information High Ground: Cyber War.” Lecture. Air Command & Staff College, Maxwell AFB, AL, 8 February 2018.

Jabbour, Kamal, Ph.D. and Muccio, Sarah , Ph.D.. "The Science of Mission Assurance." Journal of Strategic Security 4, no. 2, 2011.

Jamieson, Lt Gen VeraLinn, Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance, Headquarters US Air Force. Address. Air Force Association Air, Space & Cyber Conference, National Harbor, MD, 18 September 2017.

Kosiak, Steven M. *Arming the Heavens: A Preliminary Assessment of the Potential Cost and Cost-Effectiveness of Space-Based Weapons*. Washington, DC: Center for Strategic and Budgetary Assessments, 2007.

L3 Technologies. “LPD/LPI/AJ (LLAN) Program, ‘Final Report,’” 2 October 2017.

Lima, Bryan, Program Director for Manned C2 ISR, Northrop Grumman Aerospace Systems. Address. Air Force Association Air, Space & Cyber Conference, National Harbor, MD, 18 September 2017.

Link 16 Operational Overview. Somerset, UK: Horizon House.

Miller, Julie., Lockheed Martin. “Synergistic Full Spectrum Operations.” Briefing, digital slides, 25 January 2018.

Owens, Katherine. “Lockheed enterprise computer connects older aircraft with F-35s.” *Defense Systems*, 7 Jun 2017. https://defensesystems.com/articles/2017/06/08/lockheed-drone.aspx.

Mabrouk, Elizabeth. “What Are SmallSats and CubeSats?” *NASA*, 7 August 2017. https://www.nasa.gov/content/what-are-smallsats-and-cubesats.

Mattis, Hon. James N., Secretary of Defense. Address. Air Force Association Air, Space & Cyber Conference, National Harbor, MD, 20 September 2017.

Microsemi. “Portfolio of High-Performance Rubidium Oscillators.” 2014. https://defensesystems.com/articles/2009/07/08/defense-it1-radar.aspx.

Nelson, Capt Mary Nelson, AFLCMC/HNJ. “Project Hunter Speaker Series.” Briefing, digital slides, 22 August 2017.

Orwig, Jessica. “The Amount of Space Junk Around Earth Has Hit a ‘Critical Density’ – And It Could Jeopardize Our Space Missions,” *Business Insider*, 23 September 2015. http://www.businessinsider.com/space-junk-at-critical-density-2015-9.

Raymond, Gen John W., Commander, Air Force Space Command. Address. Air Force Association Air, Space & Cyber Conference, National Harbor, MD, 19 September 2017.

Schultze, Staff Sgt. Jeffrey, 9th Reconnaissance Wing Public Affairs. “U-2 makes first appearance during Northern Edge 17.” *Pacific Air Forces News*, 19 May 2017. http://www.pacaf.af.mil/News/Article-Display/Article/1187347/u-2-makes-first-appearance-during-northern-edge-17/.

Stone, Adam. *Embracing Software-Defined Networking: How to Overcome 4 Critical Management Challenges in Virtual Networks*. C4ISR & Networks editorial white paper. www.C4ISRNET.com/wp/virtualnetworks.

Sun Tzu. *The Art of War*. Translated by Lionel Giles. Blacksburg, VA: Thrifty Books, 2009.

United States Air Force. *Air Force Future Operating Concept: A View of the Air Force in 2035,* Sep 2015. http://www.af.mil/Portals/1/images/airpower/AFFOC.pdf.

——. *Air Superiority 2030 Flight Plan: Enterprise Capability Collaboration Team*, May 2015. www.af.mil/Portals/1/.../airpower/Air%20Superiority%202030%20Flight%20Plan.pdf.

Weeden, Brian and Victoria Samson. *Global Counterspace Capabilities: An Open Source Assessment*. Washington, DC: Secure World Foundation, 2018.

Weisgerber, Marcus. “US Air Force Is Moving Faster on Space Contracts, Industry Execs Say.” *Defense One*, 17 April 2018. https://www.defenseone.com/business/2018/04/air-force-faster-satellite-contracts-industry/147531/?oref=d-river&utm_source=Sailthru&utm_medium=email&utm_campaign=EBB%204.18.18&utm_term=Editorial%20-%20Military%20-%20Early%20Bird%20Brief.

Wikipedia, s.v. “Mesh Networking,” accessed 5April 2018. https://en.wikipedia.org/wiki/Mesh_networking

Wilhite, Tamara. “An Introduction to Software Defined Antennas.” *TurboFuture*, 8 January 2018. https://turbofuture.com/industrial/An-Introduction-to-Software-Defined-Antennas.

Wilson, Hon. Heather A., Secretary of the Air Force. Address. Air Force Association Air, Space & Cyber Conference, National Harbor, MD, 18 September 2017.

Wireless Innovation Forum. “What is Software Defined Radio?” 2017. https://www.wirelessinnovation.org/Introduction_to_SDR.

Yasin, Rutrell. *Next-Generation Communications: What Network Services 2020 and Global Network Services Will Mean for You*. C4ISR & Networks editorial white paper. www.C4ISRNET.com/wp/NextGenTelecom.

Zanjireh, Morteza M. and Hai Larijani. *A Survey on Centralised and Distributed Clustering Routing Algorithms for WSNs*, conference paper. Glasgow, UK: School of Engineering and Built Environment, 2015.