AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

DEFENDING AN AREA WITH AUTONOMY

Autonomous Intelligence, Surveillance, and Reconnaissance Capabilities leveraging Unmanned Aerial Systems for defending Forward Operating Locations

by

Edward W. Talley, Maj, US Air Force

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Dr. John P. Geis II

8 May 2017

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 US government, the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Table of Contents

Figures and Tables

Abstract

Developing UASs with autonomous capabilities will enhance local persistent ISR for defending a forward operating location against emerging threats in the 2025 timeframe. These threats will challenge current US C2ISR advantages by being faster, harder to detect, more maneuverable, have greater destructive power, disrupt communications, have greater reach, and create contested operating domains. This future operating environment increases demand for local persistent ISR such that a forward area can detect, identify, and respond to threats in a timely manner to protect friendly forces and sustain operations. UASs with autonomous capabilities present a viable means to fill this demand for increased ISR while overcoming current system limitations brought about by emerging threats and a contested future operating environment. The three proposed UAS concepts included integrating autonomy into current RPA platforms, developing new platforms with modular payloads or adaptable mission sets, and developing a platform designed to support tactical Battle-Management C2 operations. These solutions illustrate how UASs with autonomous capabilities can extend a FOAs defense network of sensors and C2 by physically increasing range, allowing more time to react, as well as improving data processing and exploitation, saving time to execute the kill chain.

Introduction

The nature of warfare is forever changing as technology evolves and new threats emerge challenging current United States (US) Command, Control, Intelligence, Surveillance, and Reconnaissance (C2ISR) advantages while placing forward deployed forces in greater risk. Prior to WWI, European countries falsely assumed that new technologies would lead to quicker wars or deter them but what they found is the nature of warfare also changes.[1] War is forever evolving and militaries must exercise caution if relying too heavily on specific technologies or simply applying new technology to the same strategies without first examining how those changes will affect the nature of warfare. Just as the advent of mechanization transformed warfare of the day, so too will fast networks, autonomy, compression of time, access to space-based capabilities, and a multitude of new lethal and non-lethal weapons.[2] From these transformations, new threats emerge to Forward Operating Areas (FOA) designed to challenge US C2ISR advantages thereby degrading operations and force protection in the 2025-2030 environment. Threats will be faster, harder to detect, more maneuverable, have greater destructive power, challenge space-based capabilities, disrupt communications, and have greater reach. Simply put, the nature of warfare is changing such that past advantages will become contested in the future. This future operating environment increases demand for persistent local ISR such that a FOA can find, fix, track, target, engage, and assess (F2T2EA) threats in a timely manner to protect friendly forces and sustain operations.

This research examines the future operating environment, identifies current system limitations, then considers the utility of using autonomy in a family of three Unmanned Aerial Systems (UAS) concepts as a means for adapting to the changing environment. To address emerging threats and overcome current system limitations, UASs with autonomous capabilities present a viable means to enhance local persistent ISR for defending a FOA. Unfortunately, the

ability of current systems and processes to provide local persistent ISR in the future operating environment is limited by a dependency on space, number of available assets, or not having the necessary range and detection capability. To mitigate these limitations the USAF can leverage upcoming autonomous technologies in the form of three proposed UAS concepts, part of a family of systems. These concepts include integrating autonomy into current Remotely Piloted Aircraft (RPA) platforms, developing new platforms with modular or adaptable mission sets, and a platform designed to support Battle Management-Command and Control (BMC2) operations. This research concludes if challenges and risks associated with autonomous capabilities are mitigated throughout the system's lifecycle, then the proposed UAS concepts are a feasible means to improving persistent ISR for the defense of a FOA in the future operating environment.

Human-Machine Team Levels of Control

Direct, automated, and autonomous are three very broad levels of control that describe decision-making responsibilities for the human-machine team. Direct control is simply a human operator in complete control of the system at all times and is responsible for all of its operations and decision-making. The system or machine cannot operate without human input. Automated is where the human operator maintains overall control of the system but delegates tasks for a machine to perform using predefined conditions. Once programed, these systems react to situations using conditions such as 'If-Then' statements. The level of automation corresponds to number of predefined conditions and the workload required of a human operator, the higher the automation the more tasks the machine can perform. Even in systems with very high levels of automation, they are limited to predefined conditions and responses keeping their decisions reactionary.[3] Autonomy then enables machines proactively make decisions and respond to the unexpected.

In systems with autonomous capabilities, the human operator defines the overall mission and the machine executes functions without dependency of human interaction by making reactive and proactive decisions for ill-defined situations. While executing its defined mission or task, autonomous decision-making can react to predefined or unanticipated events by changing behavior to best respond to the situation.[4] They can also proactively respond by analyzing and predicting changes to the threat environment, status of friendly forces, weather, or other factors.[5] Together this makes autonomy both reactive and proactive. To accomplish this, systems with autonomous capabilities learn directly from stimuli in a training environment then use this to make associations and decisions based on context.[6] Overall, autonomous technology holds high potential for not only expanding the utility of unmanned systems but also enabling operations in environments where direct human control is not physically possible.[7] Environments such as space, highly contested areas, or in the depths of the sea all present challenges for direct human control where autonomy can bolster capabilities or enable new capabilities for operations.

"Recognizing that no machine–and no person–is truly autonomous in the strict sense of the word," this research advocates machines with autonomous capabilities rather than pure autonomous systems.[8] That means a human operator is still necessary to make mission assignment and tasking decisions as well as provide guidance to the machine. Figure 1 below provides an illustration of the levels of control and decision-making responsibility in the human-machine team.

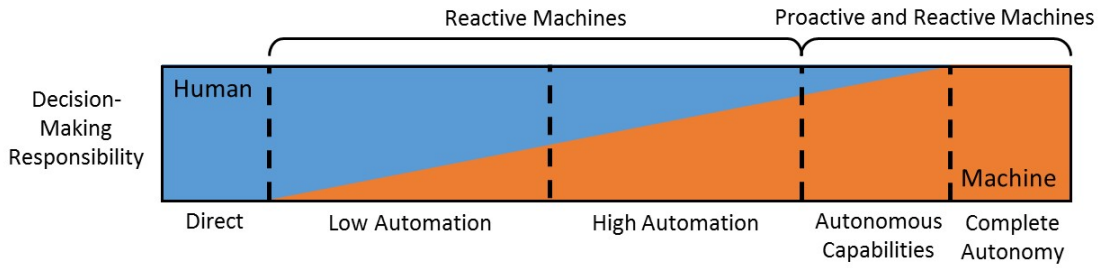

Figure 1 Human-Machine Team Levels of Control

Artificial Intelligence (AI) and Algorithms – As autonomy describes a level of control where machines are increasingly capable of decision-making, AI and algorithms then are the foundational tools that make it all work.[9] AI is the science and engineering of making intelligent machines that are able to perform tasks that would otherwise require cognitive functions of a human.[10] Such cognitive functions include learning, decision-making, reasoning, and solving ill-defined problems in complex real world situations.[11] Algorithms are the techniques and methods used to provide systematic instructions to a computer.[12] Essentially, they are the content of any computer program or the makeup of AI. As algorithms improve, they will allow AI to perform higher levels of cognitive functions. Some industries and technology sectors consider this a race to create better algorithms for AI cognitive functions that support autonomous applications. Current applications of AI include speech recognition, language translation, visual perception, self-driving cars, and strategic level game competition such as AlphaGo.[13]

Problem Overview

Future Threat Environment

FOAs in 2025 will face advanced threats designed to directly or indirectly degrade or destroy military operating capability while challenging US ISR advantages. This section will discuss both the direct threats against a specific base, as well as the indirect threats to US ISR systems. In both cases, these threats include new technologies and advanced weapons that make protecting US forces increasingly difficult since there will be little time available to defend.

Direct Threats – Growing direct threats include hypersonic weapons, technology advancements to current threats including cruise missiles and small UASs, cyberspace capabilities, and High Powered Microwaves (HPM).

Hypersonic missiles or glide rockets, defined as moving in excess of Mach 5, present one kinetic threat that will be very fast and possess the capability to perform high rate maneuvers that will make them difficult track and intercept.[14] Achieving this speed is not new, having been demonstrated in the past by intercontinental ballistic missile reentry at Mach 25 in the 1950s and then by the manned X-15 in 1961 at Mach 6.[15] Recent advances have helped modern hypersonic weapons more precisely navigate by enabling the weapon to receive GPS navigation signals in spite of the plasmas that form on the exterior of the weapons during flight. This improved precision allows for more conventional or non-nuclear options, especially lower yield and collateral damage warheads, in a long range, high speed, maneuverable, and non-ballistic flight path weapon.[16]

Today's airborne or land-based threats will still exist but as their technologies improve so will lethality and difficultly to intercept. These threats include strikes conducted by long-range bombers, low observable aircraft, advanced UASs, precision guided rockets-artillery-mortars-missiles (G-RAMM), personnel or vehicle land assault, or nuclear-chemical-biological weapons. For example, low observable, highly maneuverable, and smart cruise missiles may not be as fast as hypersonic weapons but are capable of producing similar effects. "Smart" means they have the ability to recognize countermeasures or interception attempts then evade. Other rising direct threats include hard-to-detect small UASs which can be developed to operate as swarms capable of overwhelming sensors and conducting strikes. One such technology that will increase lethality of these threats is autonomy as machines will be more capable of responding on their own to dynamic events and countermeasures. Other advances include improved aircraft or missile motors, high-density/high-discharge-rate nano-manufactured batteries, stealthy designs, and higher yield warheads amongst others.

There are also direct threats with non-kinetic approaches such as weapons employed using cyberspace. Targeted cyber-attacks on a base network could degrade internal and external C2ISR information. A targeted cyber-attack using a zero-day exploit or other malicious code could disable weapon systems.[17] The cyber domain can also facilitate messages or psychological operations to demoralize personnel or delegitimize leadership.

Another direct non-kinetic threat by 2025 is HPM weapons that can destroy or temporarily disable unshielded electronics.[18] These weapons are designed to disrupt, degrade, or destroy a target dependent on electronics by overwhelming the target's ability to reject or disperse the incoming RF energy.[19] The HPM weapons RF energy generates a strong electromagnetic field which either causes physical destruction, the overheating and melting of components, or excessive electrical stimulation that the target cannot compensate for resulting in data loss, unresponsiveness, equipment shut downs, or other effects.[20] Such an HPM weapon could be truck mounted and parked just outside a base or employed as a cruise missile for long-range strike. One example is the USAF's operational Counter-electronics High Power Microwave Advanced Missile Project, or CHAMP, however potential adversarial nations are also investing in this technology. As electronic circuit boards are in just about everything from fuel transfer pumps, vehicles, guided munitions, aircraft, and power stations, an HPM weapon would cripple a base leaving few assets operational. Due to procurement costs most systems are unshielded, those few that remain operational either had shielded electronics, were out of the blast area, under a shielded structure, or do not rely on electronics for operations.

Indirect Threats – Where direct means will target a specific base and its capabilities, indirect means will seek to accomplish similar effects to degrade operations or disable assets by

targeting space, electromagnetic (EM) spectrum, cyberspace, and air domain access and dependencies.

Access to space-based assets is necessary to provide and share C2ISR information in the defense of a FOA but challenged by emerging laser, missile, and cyber threats. A FOA depends on satellite systems for extended C2ISR sensor and communication networks, global precise navigation and timing (PNT), ballistic missile warning and tracking, as well as weather surveillance. While there are non-space dependent systems that can provide some of these capabilities, such as weather balloons or land-based radar, beyond line-of-sight (BLOS) communications for mobile assets and PNT is highly dependent on vulnerable satellites. For instance, without BLOS communications, information sharing between mobile C2ISR, strike platforms, RPAs, and joint forces will be restricted to line-of-sight (LOS) thereby degrading operations and adding substantial risk if not mitigated using extensive relay networks in advance. This challenge to space access is made realistic thanks to emerging weapons that utilize advanced laser, missile, and cyber technologies. For instance, as laser weapons mature, their improved lethality could disrupt satellite antenna arrays for communications, blind ISR sensors temporarily or permanently, or cause damage to critical components. Developments in diode-pumped and fiber laser technologies will further advance their effectiveness and efficiency in offensive applications against space-based assets. Anti-satellite missiles and cyber-attack capabilities also pose an increasing threat to space-based capabilities by physically destroying, rendering inert or taking control of an asset. Unfortunately, forthcoming laser, missile, and cyber technological advancements prove these threats a very real challenge to assuring access to space-based capabilities.[21] Of these capabilities, not receiving external or extended range ISR sensor

information through BLOS communications reduces reaction time to threats making FOAs and the bases within them more vulnerable.

Access to the EM spectrum for communications is necessary for many of the same reasons we need space capabilities, but this spectrum is under threat from emerging electronic warfare technologies. Both LOS and BLOS radio frequency (RF) communications require access to the EM spectrum for sharing critical C2ISR information between mobile platforms and dispersed bases. Permanent bases could instead share this information over fiber or copper cables if the infrastructure already exists, however this is unlikely to apply to dynamic basing and dispersal concepts thus requiring access to the EM spectrum. Challenging this access is adversarial area jamming capabilities which can significantly degrade C2ISR communications between platforms, bases, and forces affecting FOA defensive operations if not mitigated.[22] This places significant limitations on current RPA operations and manned platforms ability to provide persistent ISR data for defending a FOA.

The growth of state-sponsored cyber forces over the next decade will indirectly threaten FOA defense by affecting the global commons and decision-making calculus.[23] Adversaries could use emerging advanced cyber warfare capabilities to disrupt, degrade, or deny use of the cyberspace global commons used for various communications to share C2ISR data from around the Area of Responsibility (AOR). This could blind forward bases that were dependent on external sensors, geographically separated data processing and exploitation, or other intelligence for force protection. Strengthening cyber defense capabilities to repel attacks and reducing reliance on external ISR sources will provide a more robust threat mitigation.

Emerging advanced Integrated Air Defense Systems (IADS) and missile technologies could restrict manned platforms and degrade C2ISR projection for defensive operations. Complex

IADS and surface-to-air missile technology advancements will increase threat ranges and probability of kill that will likely cause high value C2ISR assets to remain at safer distances. While keeping these assets at a safer distance will improve their survivability, it degrades their ability to project C2 and provide ISR over the battlespace. Improvements to current counter missile systems or investing in podded high-energy laser technologies to disrupt or destroy inbound threats are viable options but until they are incorporated, the risk to airborne C2ISR assets will continue to rise.

These direct and indirect threats are but some of the many challenges that commanders within a FOA will have to contend with to ensure force protection in 2025. Of particular interest is the ability to provide local BMC2 and persistent ISR such that forces can defend against these high-speed, hard-to-detect, and adaptive threats within contested space, EM spectrum, cyber, and air environments.

Current Systems and Process Limitations

Manned Platforms – Current manned systems used to provide local BMC2 and persistent ISR for the FOA are limited in numbers, have decreased survivability, and will struggle to perform their mission given the future operating environment threats. Airborne platforms such as the E-2 “Hawkeye,” E-3 “Sentry” AWACS, E-8 JSTARS, RC-135 “Rivet Joint,” U-2 “Dragon Lady,” and others are all Low Density/High Demand (LD/HD) assets with older technology that is very costly to upgrade. This makes it difficult for them to keep up with changing threats, such as the ability to F2T2 low observable cruise missiles, and risky to use in contested environments without severe risk to personnel and equipment. Manned LD/HD assets are also likely to be positioned at safer distances from advanced long-range IADS thus limiting their coverage area. There are transportable ground-based platforms such as the Control and Reporting Center (CRC) that

provide persistent BMC2 for an area but have limited range due to operating from the ground and with less than a dozen total force units, are also LD/HD. Extending the CRCs range to cover greater areas is possible but its supporting units would require BLOS communication links using contested space or cyber networks. Despite some of these manned platforms having received recent upgrades, such as the E-2 "Hawkeye," they will still struggle to provide C2ISR for contested FOAs in the 2025 timeframe. To reinforce this limitation, expert working groups representing North Atlantic Treaty Organization (NATO) and Air Combat Command (ACC) have already identified E-3 sustainability, capability, and survivability shortfalls and are in the process of proposing capability improvements.

Unmanned Platforms – While RPAs have proven their worth as persistent ISR platforms today,[24] their value in the future operating environment is extremely limited due to the heavy reliance on space-based BLOS communications, dependent on a persistent control link with a human operator, and ISR exploitation centers.[25] Without space, RPAs are relegated to LOS operations using a small number of local ground systems designed to support takeoff and landing. In LOS operations the locBal ground station is limited to controlling just one RPA at a time, range restricted which depending on terrain could be only five kilometers, and are unable to fully utilize all onboard sensor capabilities. Expanding airborne LOS relay capabilities using RF or laser communication technology can overcome these range limitations; however, there remains a dependency on the control link. Despite having a high level of automation, the RPAs control link is critical since they are limited to reactionary responses for predefined conditions and require human control. Thereby whenever RPAs experience an unknown situation, a human operator must decide how to act requiring constant oversight and communications. Furthermore, RPAs require a connection to the Distributed Common Ground Station (DCGS) to exploit its ISR data. This

connection is highly dependent on BLOS or cyber networks and the DCGS requires significant time to analyze the data thus not a suitable means of providing quick F2T2 data for defending a FOA against emerging threats. A move towards autonomy would remove the criticality of the control link, dependency on BLOS, and enable local processing and exploitation of sensor data.[26]

Space Assets – Space has and will continue to provide the ultimate ISR high ground but is limited in sensor quantity, requires lengthy time to process-exploit-disseminate (PED) data, and must contend with emerging threats. Similar to manned platforms and RPAs, ISR satellites are LD/HD assets in which commanders often cannot get enough of in times of war. In many cases they do not make data readily available to tactical operations, requiring a processing center to first analyze and disseminate, and are not always able to monitor the FOA due to orbital requirements.[27] As other countries start to develop anti-satellite capabilities such as the lasers, missiles, or cyber-attack techniques as previously mentioned, adversaries will be able to disrupt, degrade, take-over or deny sensors or other components.[28] This limits the ability to conduct wide area ISR and together with degraded BLOS communications, FOAs will have to rely on local sources for threat detection and tracking.

Proposed Solution: UASs with Autonomous Capabilities

To address the shortfalls as discussed in the previous section, this paper proposes the use of autonomous decision-making in UASs to provide persistent ISR such that forces can effectively defend a FOZ in the 2025-2030 timeframe. Making up this UAS solution is an air or ground-based mission Tasking, Data fusion, and Coordination Cell (TDCC) comprising of a human-machine team and three different airborne application concepts. The three airborne concepts include integrating autonomy into current RPA platforms, developing new vehicles with modular or adaptable mission-focused payloads, and a platform designed to enhance BMC2 operations.

Together the TDCC and three airborne concepts share a set of common autonomous capabilities which will be outlined at the end of this section.

UAS Tasking, Data fusion, and Coordination Cell

The UAS TDCC is a common subsystem across the three proposed application concepts made up of a ground or airborne human-machine team with autonomous capabilities responsible for managing multiple unmanned aircraft and PED ISR data from various sources. Core functions of the TDCC include assigning missions to unmanned air vehicles (UAV), overseeing machine-planning actions, providing safety of flight instructions as needed, coordinating actions between platforms, performing ISR data fusion and PED, and maintaining resiliency to malicious code. TDCC machines with autonomous decision-making and high automation capability will perform most of these functions to reduce the need for a large human operator footprint. For example, a couple of human operators could simultaneously manage multiple UAVs performing local area ISR. Other autonomous capabilities these machines should possess include the following: common decision-making algorithms, environmental agility, and be trainable or have the ability to learn. Specific details regarding these capabilities are contained in the following sections. Human operators will then act as TDCC managers responsible for assigning missions and overseeing multiple UAVs, directing actions that require input or overriding machine responses, and approving threat identification and forwarding.

Airborne Application Concepts and Capabilities

RPA Assimilation – The first concept is to leverage already developed RPA platforms such as the RQ-1 Predator and integrate autonomous capabilities designed to provide persistent local ISR for FOA defense with the intent to reduce development costs and time. Depending on

the FOA's size and requirements, there could be multiple UAVs operating at once managed by a single TDCC. Figure 2 below provides a high-level concept of operations (CONOPS).

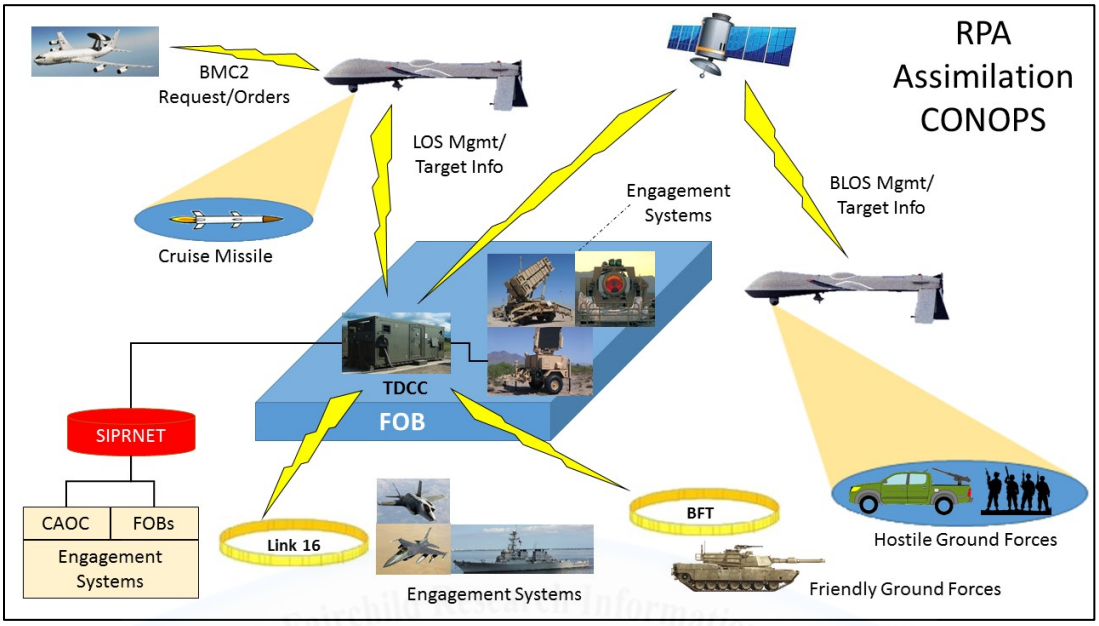

Figure 2 RPA Assimilation CONOPS

For this concept to be achievable, UASs will require the following autonomous capabilities: mission planning and dynamic replanning, safety of flight, coordination with human controllers, environmental agility, machine learning, malicious code resiliency, and data processing and reduction. These capabilities include operating in both LOS and BLOS environments as well as mitigating effects caused by a contested EM spectrum. The following paragraphs will describe each of these autonomous capabilities in more detail.

Capability #1: Mission Planning and Dynamic Replanning – The future operating environment will experience lower-quality communication links requiring UASs to possess mission planning and dynamic replanning capabilities using a layered decision-making approach similar to that of deep-space vehicles.[29] Core requirements include developing a well-defined mission plan, executing the plan and modifying it if necessary, reacting to irregular events, and coordinating with human operators and are critical for autonomous decision-making. For machines

to accomplish this, researchers have developed a layered approach that enables a responsive and robust architecture to address autonomous decision-making challenges using various timescales.[30] Figure 3 and the discussion below provide a common architecture that has been adapted for UAVs and has three layers of autonomous control: deliberate planning, execution, and reaction.[31]

Deliberate planning, the highest layer of control, uses models of the mission, environment, and system combined with current state information from the execution layer to develop plans and determine if the current situation requires dynamic replanning.[32] Parameters found within these models include ROEs, threats, airspace corridors, prioritized target listing, mission taskings or requirements, kill boxes, communication plans, friendly force data, platform specifications, and so on. These models are to be provided prior to launch but can be modified during the mission in order respond to dynamically changing conditions.

The execution layer's purpose is to provide behavioral inputs, monitor events that would trigger the execution of a contingency plan, and request replanning in the event there are no matching courses of action (COA).[33] Until a new plan is developed, the execution layer executes the best COA on hand. Events that could trigger a contingency plan may include significant changes to the threat environment or alternate communication methods.

The lowest layer of control is reaction, named for its fast deterministic responsiveness, and is especially useful in providing safety of flight. Since speed is the key attribute of the reaction layer it performs similar to automated control where all conditions are predefined.[34] Maintaining flight and mission safety is a chief concern for this layer so constant monitoring of the operating environment using sensors and communication equipment, vehicle flight dynamics and subsystem status, and the ability to coordinate with human controllers are necessary. Safety of flight and coordination are important enough to list out as separate critical capabilities.

Operating asynchronously, the layered decision-making approach has proven its feasibility where direct human control is limited. All three layers in this approach operate asynchronously in parallel to produce optimal behavior and have different responsiveness due to complexity of decision-making.[35] Similar architectures have already been widely implemented in autonomous systems such as underwater vehicles and exploratory spacecraft with expansion into intelligent manufacturing systems.[36] While this layered architecture illustrates an UAV application, a similar construct can be beneficial for TDCC autonomous decision-making capabilities.

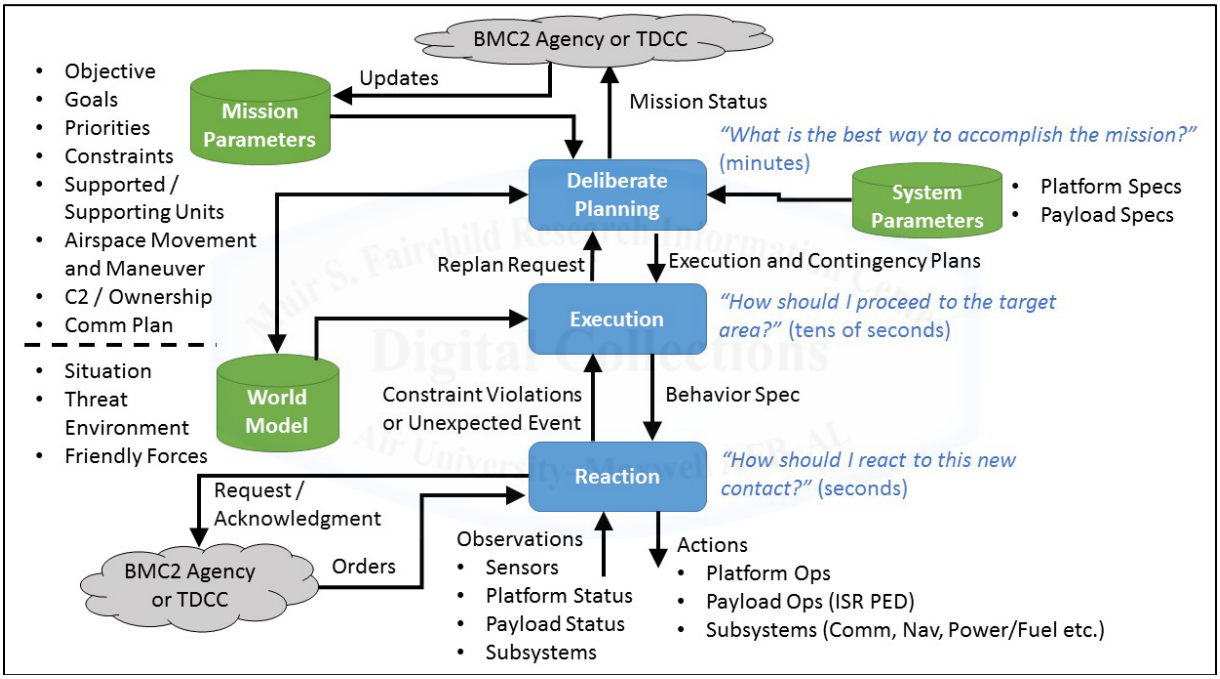

Figure 3: Autonomous UAV Layered Decision-Making Architecture

Capability #2: Safety of Flight – The autonomous UAS will be required to monitor, decide, communicate, and maneuver to maintain safety of flight and avoid airspace collisions. Safety of flight occurs primarily onboard the UAV with the TDCC providing instructions as needed.

Capability #3: Coordinate with Human Battle Managers and ATC – UAVs operating with autonomous capabilities and not dependent on constant supervision must be able to coordinate with human battle managers and air traffic controllers (ATC). This includes accepting commands,

mission changes, retaskings, direction, and airspace control from various sources. Sources include BMC2 agencies, a manned flight lead, airfield operations, ATC, or the TDCC. These changes or direction can come in the form of digital data or verbal speech in which the UAV must be able to understand, react, and acknowledge. Coordination also includes the ability to update human controllers on its mission status or critical threat information to itself or others.

Capability #4: Environmental Agility – Using autonomous decision-making algorithms allow a UAS to have communication and navigation agility within a contested operating environment with minimum human involvement. One example is being able to operate within a contested space environment, which include Global Positioning System (GPS) or BLOS communication degradation or denial. In the event GPS becomes denied or degraded, the UAV should decide how to best navigate based on the situation. This could include using a variety of sources such as Inertial Navigation Systems (INS), terrain recognition, beacons, celestial, other space-based navigation satellites, or if feasible and necessary, altering course to maintain GPS lock. In a contested RF environment, since an autonomous system does not require a human control link, it can continue to operate and preform its assigned mission whether it maintains contact with its TDCC or not. The system could then decide how best to act to accomplish its tasks by analyzing the situation, rules of engagement, mission importance, and other factors. For example, the UAV could autonomously switch means of communication, such as optical or another frequency, and if it determines that local supported forces are able to receive communications then it could stay on station. In the event all means of communications are jammed, it could reposition to reestablish contact, continue to perform the mission storing ISR data locally for later dissemination, or some combination thereof based on the mission and situation. Worst case the UAV could decide the best COA is to return to base using an alternate navigation source. Another example is the ability to

operate within a contested air domain. If the UAV detects or is alerted to an air threat it would need to make a decision to stay on station thereby relying on countermeasures and tactics, relocate to a safer position, or weave in and out of the threat range to collect the necessary ISR data.

Capability #5: Trainable – Autonomous algorithms and AI technology must have the capability to learn directly from training stimuli, make associations based on context and their experiences, and ideally share learned behavior within their family of systems.[37] As the systems receive training and operational experiences, their performance and decision-making will improve. This training however can take considerable time and as research concerning machine neural nets show, a human or machine trainer is required for verification before the event is actually learned.[38] Today autonomous systems learn from training data and sentiment analysis but in the near future will be able to learn by doing and watching.[39] Compressing training time to just weeks is possible as practices improve but of particular utility is the sharing of learned behavior amongst UASs with the help of common decision-making algorithms.[40] Applying what one UAS learns to others will thereby expedite decision-making progress and knowledge sharing across a family of systems.

Capability #6: Resiliency to Malicious Code – Unmanned systems operating in future threat environments need to be resistant and able to protect against cyber intrusion and exploitation attempts. This includes protection measures throughout development, production, training, operations, and sustainment. Providing robust cyber defense onboard a UAV is more of a challenge than in larger ground systems because of physical space limitations, decreased ability make hardware alterations, and less available processing power though rising computing capabilities help. At minimum, the UAV should be able to identify the intrusion attempt then either defeat and revive the affected subsystem or isolate it such that malicious code cannot spread.[41]

Capability #7: Onboard Sensor Processing and Data Reduction – To provide ISR for FOA defense, the RPA Assimilation concept will require the use of radar and electro-optical/infrared (EO/IR) sensors as well as onboard data processing to identify and track targets while providing initially processed threat information. Leveraging technology already in development by Air Force Research Lab's Hyper/multispectral Data Reduction and Archiving (HyDRA) program will allow the UAV to positively identify and track threats using video imagery while being complemented by the radar. This technology, along with a more advanced active EO/IR sensor pod, is forecast to mature within the next five years.[42] The UAV would then send target identification, supporting sensor imagery such as a picture or short video clip, and tracking data to the TDCC for verification and integration with other sensors. Initial onboard data processing and reduction not only decreases communication bandwidth requirements but also decreases the amount of data the TDCC must process thereby improving its overall performance in providing timely results. If necessary, the TDCC could request a live active sensor feed by reallocating bandwidth with other platforms.

Capability #8: Consolidated Data Fusion and Forwarding – The TDCC will serve as the node responsible for fusing data from multiple sources, verifying threats, and forwarding refined target data to engagement platforms and HHQ. Once the TDCC has the target information, the human-machine team can correlate the tracking data with other airborne or ground sensors, perform additional processing and interpreting, and verify the target identification. If approved by a human operator for prosecution, the TDCC will forward threat target-tracking data directly to engagement platforms such that their own sensors can establish a fix or fire off remote. To expedite matters, the TDCC could bypass its data processing routines and forward initially processed threat data it receives from the UAV with the highest track quality to the engaging weapon system. While

this is occurring, the TDCC should also disseminate critical threat information throughout the FOA and to Higher Headquarters (HHQ) such that forces can then use the data to build an operating picture for defense. For ISR data to be rapidly processed, exploited, and disseminated at a rate the 2025 operating environment demands will require the TDCC to have autonomous decision-making algorithms, heavy automation, and humans as the overseers. Figure 4 below provides an illustration of the described onboard processing, data fusion, and forwarding capabilities.

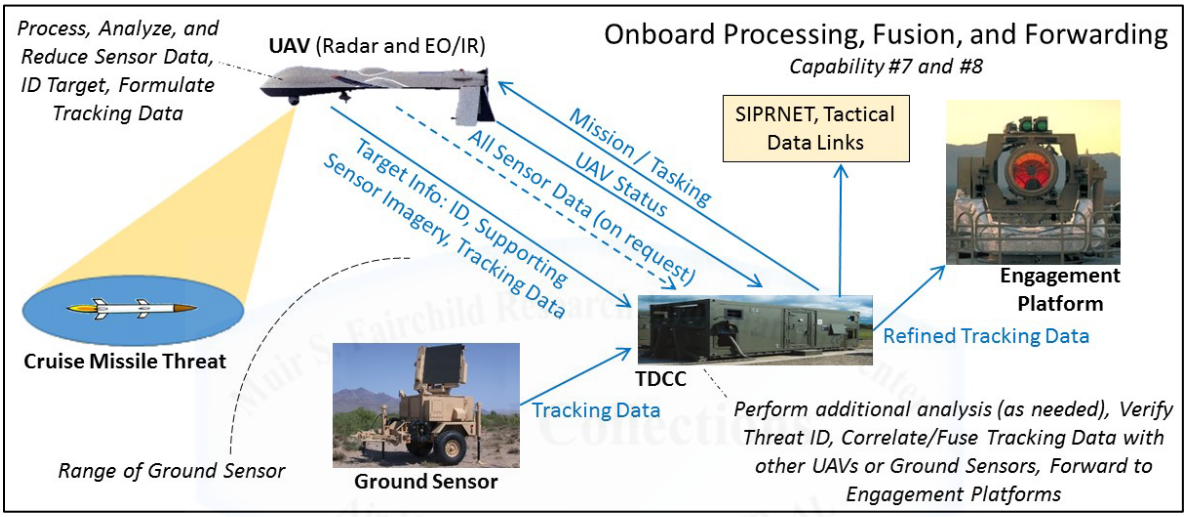

Figure 4 Onboard Processing, Fusion, and Forwarding Capabilities

Processing, fusing, and forwarding data from multiple sources in a consolidation center such as the TDCC presents greater technical maturity and robustness compared to a distributed method. Distributed ISR data fusion would involve PED across all UAVs, sometimes referred to as "cloud computing." To do this would require complex cooperative processing routines that are highly dependent on meshed communication links. By severing a link, even temporarily, there would be interrupts as the system reallocates processing and data sharing. Distributed data fusion would also require high bandwidth requirements, which are not favorable in contested RF environments. For these reasons of complexity and concept maturity when operating multiple UAVs, it is more practical in the 2025 operating environment to consolidate data fusion at the local

TDCC. Consolidating ISR data fusion adds risk associated with a single node but mitigated by adding a secondary TDCC in the FOA.

With these eight capabilities, the Assimilation concept overcomes current RPA limitations by reducing dependency on a control link and space-based BLOS, allows the operation of multiple UAVs per control node, increases agility within a contested RF environment, and is able to locally process and exploit ISR data for defending a FOA.

Overwatch – The second concept, Overwatch, builds upon the RPA Assimilation concept by utilizing different air platforms with modular sensor payloads to provide local ISR for FOA defense. These platforms can vary in size and type, fixed wing or rotor, depending on the designed employment environment but the intent is to maximize the use of open architecture interfaces with the TDCC and modular payloads.

Capability #9: Modular Payloads – Modular payloads allow threat-focused employment, maximizes space for better sensors of the needed type, and improves adaptability to new or changing threats. For example, instead of trying to pack multiple sensors into a single integrated platform they can be broken up into modular payloads such that there can be more space for increased mission type capabilities. Payloads could include various types of radars, EO/IR sensors with or without laser designation, signals intelligence (SIGINT), communication or tactical data link (TDL) relays, directed energy weapons such as a counter-missile high energy laser, hyper-spectral imaging, and so on. Modularity and open architecture designs are also more adaptable to emerging threats compared to an integrated solution. Instead of having to develop a new platform or undergoing significant changes to respond to a threat, a single payload could be developed or modified then inserted into the air vehicle using standard interfaces.

The modular concepts and autonomous technologies proposed in this Overwatch concept are not far away; in fact, other countries have already made developmental progress. For example, Israeli manufacture Elbit Systems' makes the Hermes 900 that provides a modular and open architecture design with autonomous capabilities embedded within the ground station. The Hermes 900 is not a large unmanned air vehicle but allows for an 8.2-foot modular payload length[43] weighing a little over 770 pounds.[44] They advertise payloads with such capabilities as advanced EO/IR, various types of radar, SIGINT, electronic warfare jamming, EO mapping and surveying, hyper spectral, and wide area persistent stare.[45] Hermes 900 as well as its smaller 400 variant includes an intelligent management center with similar autonomous capabilities as the proposed TDCC to include multiple UAV management from a single station, data fusion and forwarding, and what the company calls "highly autonomous" decision-making.[46] Its autonomous decision-making capabilities include mission management and UAV flight operations allowing a human operator to oversee multiple UAVs and monitor sensor data.

Figure 5 Hermes 900 with Modular Payloads
(top: payload illustrator; left: wide-area EO/IR with data processing-exploitation; right: radar)

Capability #10: Independently Forward Threat Data to TDL Networks – While modular payloads allow adaptability in future operating environments these subsystems should also utilize autonomy to conduct onboard processing allowing the Overwatch concept to publish threat data

directly to TDL networks to expedite the kill chain. As discussed with the onboard processing and data reduction capability these initial actions within the payload saves communication bandwidth and time for the TDCC to fuse data across multiple platforms. This initial processing also enables certain Overwatch platforms to publish processed ISR data, independent of the TDCC, directly to local TDL networks as long as the information meets predefined qualifiers thereby speeding up the kill chain. Local TDL networks include Link 16, Link 22, Blue Force Tracker (BFT), Fighter Data Link, or other joint interface. Figure 6 below provides a high-level Overwatch CONOPS.

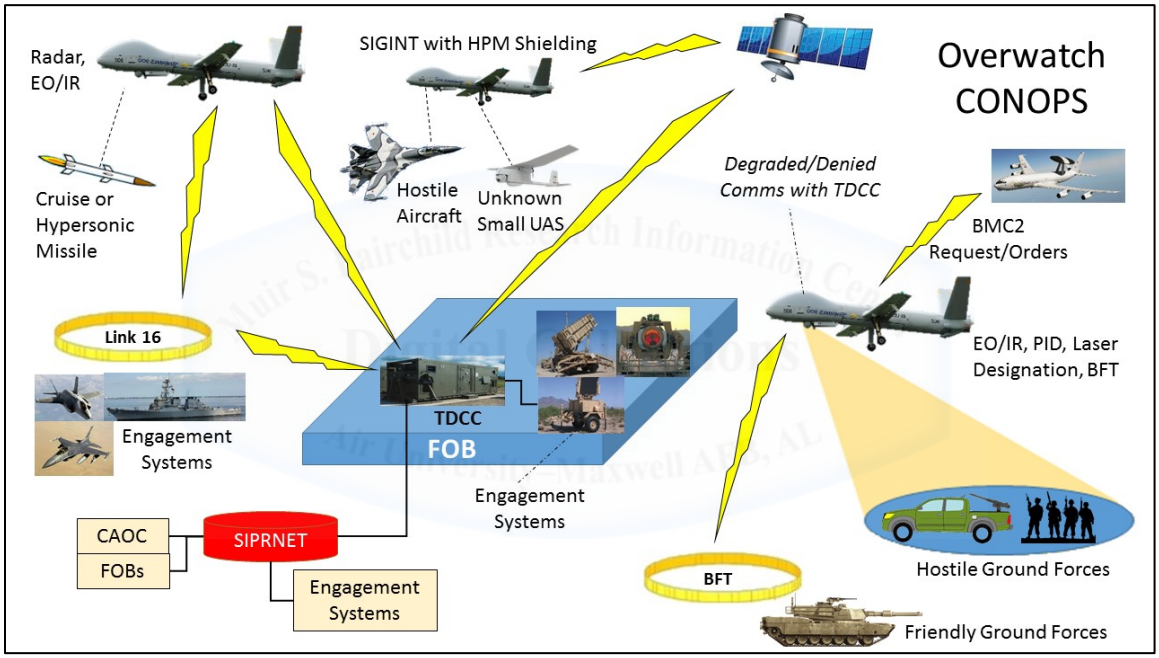

Figure 6 Overwatch UAS CONOPS

Capability #11: HPM Shielding – As directed energy HPM weapons become more prevalent in the future operating environment, measures will need to be taken to shield critical UAV and TDCC electronic components. Fully shielding all UAVs against HPM is cost prohibitive and not necessary for every mission therefore a mix of protection levels would best balance costs and necessity. Such levels could include full HPM shielding, protecting only the critical components and circuits, or no shielding depending on the UAV platform type and intended

purpose. The TDCC on the other hand should at least have its critical electronics shielded if not the entire systems to maintain mission management, data fusion, and target forwarding functions.

BMC2 Extension – The third concept utilizes an UAV designed to extend sensor and communication coverage for airspace BMC2 weapon systems such as the AWACS, JSTARS, CRC, or USMC's Tactical Air Operations Center. Due to the array of electronic equipment required for BMC2 this platform is likely to be on a similar scale to a RQ-4 Global Hawk or larger. Unlike the Overwatch's modular payload capability, the BMC2 Extension will likely need to integrate multiple types of sensors and communications equipment in order to fulfill its mission. NATO's "alliance future surveillance and control solutions working group" has already identified a concept similar to this as their preferred method of modernizing AWACS capability to meet threats within the 2025-2035 timeframe.[47] Their concept includes a modernized E-3 fleet capable of leveraging the use of UASs as sensor and communication extenders much like the proposed BMC2 extension.[48]

Capability #12: Support and Extend Airspace BMC2 Defense Network – The capability to support and extend airspace BMC2 leverages a variety of sensors, communications, and processing equipment to create a more robust FOA C2 network by increasing range and keeping LD/HD manned platforms at safer distances. The UAV would need to be equipped with radar, SIGINT, voice and data communications, radio relay, TDLs, sensor processing, and subsystem supervisory control with autonomous decision-making. Supervisory control with autonomous capabilities would allow the platform to adjust and adapt its various subsystems to environmental or situation changes. Overall BMC2 tactics, techniques, and procedures over the FOA will still require a manned platform where the TDCC function should reside. For example, a future AWACS could use these UAVs to provide coverage over a higher risk area thereby allowing the manned

crew to remain at a safer distance. A flexible configuration would allow the UAV to either pipe its radar data and communication links to the AWACS for correlation and processing, or publish track data directly to a TDL depending on mission requirements. Without its manned BMC2 platform, this UAV could also serve independently much like those described in the Overwatch concept. In this role, the UAV could provide its sensor data and communication links to another TDCC or publish track data directly to a TDL network so long as the information meets predefined qualifiers.

Another use for this concept could be in operating environments like Afghanistan where rugged terrain obstructs sensing and communication. Here the USAF had to leverage manned and unmanned versions of the Battlefield Airborne Communications Node (BACN) to provide reliable voice communications and TDLs for the operating area. Without this capability, the TDL and airspace control communication networks would have been significantly degraded.

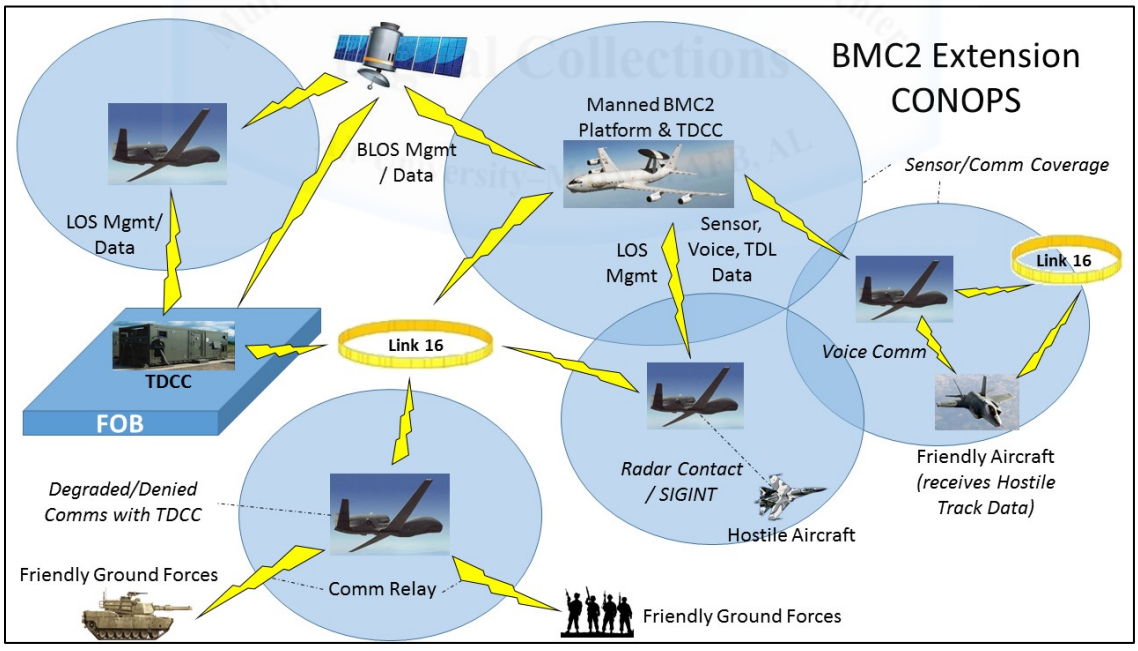

Figure 7 BMC2 Extension CONOPS

Overarching Autonomous Capabilities

As a family of systems, the TDCC and the three airborne concepts will share certain critical autonomous capabilities that enable them to perform their mission with minimal need for human

control in a contested environment. The first is common decision-making algorithms and AI that serves as foundational to all other autonomous capabilities.

Capability #13: Common Decision-Making Algorithms and AI – Having common autonomous decision-making algorithms and AI for UAS operations will optimize developmental efforts, saving cost and time but platforms would still maintain a degree of complexity challenging adversarial attempts to exploit. Common algorithms allow researchers to focus developmental efforts thereby removing duplicative monetary investments and increasing the potential of earlier product maturity. In terms of acquisition speak – reduced costs and schedule. There is also a higher potential for maximizing algorithm performance, as this would increase the collaboration and knowledge sharing amongst researchers. Having applicability across multiple platforms would also reduce the sustainment footprint by having less to maintain as well as by consolidating machine learning and training constructs. A notable disadvantage for having common decision-making algorithms is that an adversary could focus their exploitation efforts. This is a concern but the adversary would still face multiple platforms each having their own unique level of complexity due to different subsystems, modifiable operating environment models, and mission dependent parameters. For example, some algorithms will be subsystem specific such as those used for navigation, communication, power, and sensing.[49] The mission planning and dynamic replanning capability further depicted these complexities with various inputs to its layered architecture.

Capability #14: Autonomous Group Coordination – Autonomous group decision-making algorithms seek to coordinate actions between multiple systems for accomplishing a single purpose and should be performed at a central node instead of across platforms to reduce technical risk. Commonly referred to as swarm intelligence, this research seeks to emulate the social behaviors found with foraging ants, flocking birds, or a wolf pack hunting.[50] Replicated in the past without

an explicit coordination plan or global communications proves this behavior has potential.[51] To decrease technical maturity and risk, current swarm implementations focus on homogeneous systems, minimal decision-making using predefined rule sets, implicit C2, and low levels of human-machine interaction.[52] However, swarm intelligence becomes more complex if trying to leverage autonomy's ability to respond to unanticipated situations due to distributed group decision-making,[53] integrating heterogeneous systems, having complex reasoning, or requiring a high level of human-machine interaction.[54] This distributed implementation makes not just the algorithms more complex but creates additional sensing and communication requirements.[55] To reduce design risk and ensure technological maturity, group coordination should be restricted to a central node such as the UAS TDCC. The TDCC would monitor the FOA situation using all sensor platforms and issue retasking orders as needed. As group coordination and swam intelligence technologies mature this capability can move from a centralized to distributed application.

#	Capability	Assimilate RPA	Overwatch	BMC2 Ext.	TDCC
1	Mission Planning and Dynamic Replanning	X	X	X	Manage
2	Safety of Flight	Primary	Primary	Primary	Alt
3	Coordinate with Human Bat. Manager/ATC	X	X	X	X
4	Environmental Agility	X	X	X	X
5	Trainable	X	X	X	X
6	Resiliency to Malicious Code	X	X	X	X
7	Onboard Sensor Processing/Data Reduction	X	X	X	
8	Consolidated Data Fusion and Forwarding				X
9	Modular Payloads		UAV and Payload Dependent		
10	Independently Forward Data to TDL Nets			X	
11	HPM Shielding*			X	X
12	Support/Extend FOA BMC2 Defense Net			X	X
13	Common Decision-Making Algorithms/AI	X	X	X	X
14	Autonomous Group Coordination				X
*Does not contain autonomous decision-making capabilities					

Table 1 Proposed Concept Capability Summary

Findings

Along with the most recognized benefit of reducing manpower requirements and risk to human life,[56] autonomous technology can improve a FOAs defense network and mitigate unmanned system limitations. This section will summarize these defense specific benefits as supported throughout this paper as well as claim autonomous technology is rapidly maturing but does maintain notable challenges.

Improves FOA Defense Network, Physically and Temporally – The proposed solutions illustrated how UASs with autonomous capabilities can extend a FOAs defense network of sensors and C2 both physically and temporally. Physically, the solutions augment ground or sea-based systems by extending sensor and communication networks using UAVs equipped with radar, EO/IR, hyper-spectral imaging, SIGINT, radio, or TDL amongst other capabilities. The UAS concepts can also augment and reduce risk to LD/HD C2ISR aircraft as well as operate without dependency on space-based communications. Reducing the demand for LD/HD air or space-based assets improves a commander's flexibility and platform utilization throughout the AOR. As recommended by Naval Air-Sea Battle Concept strategists, investing in agile UASs to provide persistent local ISR is necessary in the future operating environment to keep high-value manned platforms at safer distances and mitigate contested area challenges.[57] Temporally, autonomous decision-making capabilities can enhance onboard ISR data processing and exploitation improving the quality and speed of disseminating threat data in time-critical situations.[58] UAV payloads with autonomous capabilities can search out, identify, locate, and track threats for local dissemination to a TDL, TDCC, or weapons engagement platform. Initial onboard processing also frees up bandwidth across the spectrum for reallocation to other capabilities and allows for retransmission of threat information if communications become intermittent since a constant live data stream is

not required. Improving the range and robustness of the physical networks while decreasing the time required for executing the kill chain enhances a FOAs ability to defend against future threats.

Mitigates Unmanned System Limitations – As presented in this research the application of autonomy in UASs reduces the dependency of maintaining direct human operator control through vulnerable communication links and overcomes onboard decision-making limitations. UASs providing persistent ISR in defense of a future FOA will likely have to contend with a contested environment where space-based BLOS or LOS communications could become intermittent or denied at range. Autonomy can mitigate these communication dependencies by enhancing onboard decision-making capabilities allowing a UAV to continue with its mission or modify it based on the environment it is experiencing. Specifically, autonomy brings proactive decision-making capabilities onboard the platform that can adapt to unexpected situations whereas current RPAs are dependent on maintaining a direct link with human controllers for the same capability. UASs with autonomous capabilities will still interact with a small number of human managers but do not require constant input and direction.

Rapidly Maturing Technology – Civilian industry, academia, and government labs are already developing and fielding technologies with autonomous capabilities. Perhaps the most notable civilian accomplishments include IBM's Watson, Google and Uber self-driving cars,[59] a semi-autonomous commuter bus by Mercedes.[60] In 2014 alone, US and Japanese companies invested over $2 billon in autonomous systems.[61] Academic institutions have also invested research into autonomous control and algorithms as evident in Stanford's mobility-on-demand program.[62] As the commercial market and academia accelerate maturation of autonomy, the DoD should take the opportunity to leverage their investments wherever possible.[63] Of course, DoD and US National Labs are not sitting quietly and waiting on the commercial market. They are also

investing in autonomous research in areas spanning UASs serving as loyal wingman to manned platforms, small UAS teaming for base security and intrusion detection, sensor processing and data interpreting algorithms, combating small boat swarms,[64] and conducting undersea rescue missions just to name a few.[65] Considering these developments and in discussion with AFRL experts, it is practical to say that autonomous technology will be mature by 2025-2030 for unmanned platform operations as proposed in this research.

Challenges and Mitigations – The most significant challenges for autonomous systems include HPM weapons, trust, training, and funding. Since autonomous systems rely heavily on computer circuits, electricity, and RF signals they are extremely vulnerable to HPM.[66] Mitigation measures include properly shielding critical components using counter-HPM materials and inserting diodes that cut circuit paths such that there would be minimal mission degradation.

Many studies outline the key issues and barriers for trusting and training autonomous systems but in short, both will take time. The proposed solutions in this research require a level of trust between man and machines that does not exist today. Ways to build this trust can be complicated and demand a time intensive integrated approach across the systems lifecycle but it is achievable.[67] Just as building trust will take time, so too will training autonomous systems.[68] Once trained, their knowledge can uploaded to other systems, expediting fielding and if utilizing the proposed common decision-making algorithms can be used across multiple types of platforms.

Funding is a challenge for every program but by leveraging various industry and lab investments presents opportunities for collaboration and reduction in duplicative effort. Aside from arguing the need for more money, there are potential costs savings if the DoD can leverage investments made by the commercial industry. Certain programs mentioned in this proposed concepts such as AFRL's HyDRA are currently funded and on schedule. Others such as the

Autonomous Loyal Wingman program have funding gaps in the years to come, which will delay their maturation. While these two programs differ in research focus, there are duplicative efforts between the Navy, Air Force, US National Labs, and Army that if consolidated, would maximize funding and collaboration for autonomous system development.

Recommendations

The following are recommendations derived from this research for senior leader consideration and action regarding UASs with autonomous capabilities for defending a FOA.

- Invest in autonomous ISR processing and exploitation capabilities to improve kill chain quality and speed to overcome emerging threats.
- Develop UASs with autonomous capabilities as proposed by the RPA Assimilation and Overwatch concepts to extend a FOAs defense network without risking or tying up LD/HD manned C2ISR platforms.
- Utilize modular payloads capable of being swapped out in a timely manner and designed for a particular mission or threat environment in order to maximize physical space for necessary sensors and HPM shielding. Modularity and open architecture interfaces also allows the development of new payloads to address emerging needs without having to modify the UAV.
- Develop UASs with autonomous capabilities, as described in the BMC2 Extension concept, to work with manned C2ISR platforms extending their coverage and improving their survivability in a contested environment.
- Leverage civilian industry and academia to accelerate maturation of autonomous capabilities. Just as globalization can allow the DoD to leverage the research of the commercial market and academia so too is that information accessible to potential adversaries.[69] Therefore, the

US must accelerate its exploration into autonomy to both realize its full military value and to remain ahead of adversaries who wish to exploit its operational benefits.[70]

Summary and Conclusion

Developing UASs with autonomous capabilities will enhance local persistent ISR for defending a FOA against emerging threats in the 2025-2030 operating environment. These threats will challenge current C2ISR advantages by being faster, harder to detect, more maneuverable, have greater destructive power, disrupt communications, have greater reach, and create contested operating domains. This future operating environment increases demand for local persistent ISR such that a FOA can detect, identify, and respond to threats in a timely manner to protect friendly forces and sustain operations. UASs with autonomous capabilities present a viable means to fill this demand for increased ISR while mitigating current system limitations brought about by emerging threats and a more contested future operating environment. The three proposed UAS concepts included integrating autonomy into current RPA platforms, developing new platforms with modular payloads or adaptable mission sets, and developing a platform designed to support BMC2 operations. These solutions illustrate how UASs with autonomous capabilities can extend a FOAs defense network of sensors and C2 by physically increasing range, allowing more time to react, as well as improving data processing and exploitation, saving time to execute the kill chain.

Incorporating autonomy into unmanned systems presents its challenges but if the recommended mitigations are applied throughout the lifecycle then the proposed solutions are a viable means to improving persistent ISR for FOA defense. The most significant challenges for autonomous systems as described include technical maturity, HPM weapons, trust, training, and funding. Confronting all of these challenges will require the help of investments already made by civilian industry, academia, and government labs. In many cases, there has already been significant

research progress such as HPM shielding. Others such as developing human-machine trust and training processes will take time. If these challenges and risks associated with autonomous capabilities are mitigated throughout the systems lifecycle, then the proposed UAS concepts are a feasible means to improving persistent ISR for the defense of a FOA in the future operating environment.

Appendix A: Additional Discussion

Additional Finding: Autonomy Enables New Missions – As we move into the future, autonomous technology will also enable new missions that would otherwise be impossible.[71] This holds especially true for those operational environments where human control is not only a challenge but impossible.[72] Environments such as space, highly contested areas, or in the depths of the sea all present challenges for direct human control where autonomy can bolster capabilities or enable new capabilities for operations. For example, unmanned platforms sent into a contested area or behind enemy lines to collect critical ISR data to give friendly forces an advanced notice that an attack is imminent allowing FOAs to ready defenses.

Appendix B: Acronyms

ACC	Air Combat Command
AFRL	Air Force Research Lab
AFSC	Alliance Future Surveillance and Control
AI	Artificial Intelligence
AOR	Area of Responsibility
ATC	Air Traffic Control
AWACS	Airborne Warning and Control System
BACN	Battlefield Airborne Communications Node
BFT	Blue Force Tracker
BLOS	Beyond Line-Of-Sight
BMC2	Battle Management-Command and Control
C2	Command and Control
C2ISR	Command, Control, Intelligence, Surveillance, and Reconnaissance
CAOC	Combined Air Operations Center
CJSC	Chairman of the Joint Chiefs of Staff
COA	Courses of Action
CONOPS	Concept of Operations
CRC	Control and Reporting Center
DCGS	Distributed Common Ground Station

DoD	Department of Defense
DSB	Defense Science Board
EM	Electromagnetic
EMP	Electromagnetic Pulse
EO	Electro-optical
F2T2EA	Find, Fix, Track, Target, Engage, and Assess
FOA	Forward Operating Area
GPS	Global Positioning System
G-RAMM	Guided Rockets-Artillery-Mortars-Missiles
HHQ	Higher Headquarters
HPM	High Powered Microwave
HyDRA	Hyper/multispectral Data Reduction and Archiving
IADS	Integrated Air Defense Systems
INS	Inertial Navigation Systems
IR	Infrared
ISR	Intelligence, Surveillance, and Reconnaissance
JSTARS	Joint Surveillance and Target Attack Radar System
LD/HD	Low Density/High Demand
LOS	Line-Of-Sight
NATO	North Atlantic Treaty Organization
PED	Process, Exploit, and Disseminate
PNT	Precise Navigation and Timing
RF	Radio Frequency
RPA	Remotely Piloted Aircraft
SIGINT	Signals Intelligence
SIPRNet	Secret Internet Protocol Router Network
TDCC	Tasking, Data fusion, and Coordination Cell
TDL	Tactical Data Link
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle
USAF	United States Air Force
USMC	United States Marine Corps

End Notes

[1] Joshua C. Ramo, *Seventh Sense* (New York, NY: Little, Brown and Company, 2016), 233.
[2] Ibid., 233.
[3] Chairman of the Defense Science Board, *Summer Study on Autonomy* (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, June 2016), 4.
[4] David P. Watson and David H. Scheidt, "Autonomous Systems," *Johns Hopkins APL Technical Digest* 26, no. 4 (2005): 368.
[5] Chairman of the DSB, *Summer Study on Autonomy*, 4.
[6] Lt Col Erik C. Bowman, "Intelligence, Surveillance, and Reconnaissance Processing, Exploitation, and Dissemination System in support of Global Strike in 2035," (master's thesis, Air War College, February 2012), 11.
[7] David P. Watson and David H. Scheidt, "Autonomous Systems," 368.
[8] Chairman of the DSB, *Summer Study on Autonomy*, 5.
[9] Ibid.
[10] John McCarthy, "What is Artificial Intelligence: Basic Questions," Standford.edu, 12 November 2007, http://www-formal.stanford.edu/jmc/whatisai/node1.html.
[11] Stuart J. Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach (3rd ed.)* (Upper Saddle River, NJ: Prentice Hall, 2009), 1-5.
[12] Stephen F. DeAngelis, "Artificial Intelligence: How Algorithms Make Systems Smart," *Wired*, September 2014, https://www.wired.com/insights/2014/09/artificial-intelligence-algorithms-2/.
[13] "AlphaGo Games," DeepMind Lab, 21 January 2017, https://deepmind.com/research/alphago/.
[14] Kenneth F. Johnson, "The Need For Speed: Hypersonic Aircraft And The Transformation Of Long Range Airpower," (master's thesis, School and Advanced Air and Space Studies, June 2005), viii.
[15] John Anderson, *Hypersonic and High-Temperature Gas Dynamics Second Edition* (Reston, VA: American Institute of Aeronautics and Astronautics, 2006), 4-5.
[16] Chairman of the Joint Chiefs of Staff, *Joint Operating Environment 2035* (Washington, DC: Office of the Joint Chiefs of Staff, 14 July 2016), 19.
[17] Richard A. Clarke and Robert K. Knake, *Cyber War* (New York, NY: Harper-Collins Publishers, 2010), 89-101.
[18] Chairman of the Joint Chiefs of Staff, *Joint Operating Environment 2035*, 17.
[19] Lt Col Robert J. Capozzella, "High Power Microwaves on The Future Battlefield: Implications For US Defense," (master's thesis, Air War College, 17 February 2010), 5.
[20] Ibid., 4-8.
[21] Ibid., 32-33.
[22] Ibid., 32-33.
[23] Ibid., 7.
[24] US Air Force, *Air Force Doctrine Volume 1: Basic Doctrine* (Maxwell AFB, AL: LeMay Center, 2015), 72.
[25] Chairman of the DSB, *Summer Study on Autonomy*, 65.
[26] David P. Watson and David H. Scheidt, "Autonomous Systems," 370.
[27] Joint Chiefs of Staff, *Joint Publication 3-14: Space Operations* (Washington, DC: Office of the Joint Chiefs of Staff, 2013), V5-7.
[28] Chairman of the Joint Chiefs of Staff, *Joint Operating Environment 2035*, 32.
[29] David P. Watson and David H. Scheidt, "Autonomous Systems," 369.

[30] Ibid., 371-372.
[31] Ibid.
[32] Ibid.
[33] Ibid.
[34] Ibid.
[35] Ibid.
[36] Ibid.
[37] Lt Col Erik C. Bowman, "ISR PED System in support of Global Strike in 2035," 11.
[38] Ibid.
[39] Chairman of the DSB, *Summer Study on Autonomy*, 11.
[40] Ray Kurzweil, *The Singularity Is Near* (New York, NY: Penguin Books, 2006) 294.
[41] Chairman of the DSB, *Summer Study on Autonomy*, 92-93.
[42] US Air Force, *2015 Program Element 0603742F: Combat Identification Technology Budget Item Justification Exhibit* (Washington, DC: US Air Force Headquarters, March 2014).
[43] "Elbit Systems' Hermes 900: Equipped with Multiple Advanced Payloads," Aerospace and Defense News, 6 February 2012, http://www.asdnews.com/news-40818/Elbit_Systems__Hermes_900:_Equipped_with_Multiple_Advanced_Payloads,_this_UAS_is_Leading_its_Class_in_Multi-Mission_Performance.htm.
[44] "Hermes 900," Elbit Systems, 19 February 2017, http://elbitsystems.com/product/hermes-900-5/.
[45] "Elbit Systems' Hermes 900: Equipped with Multiple Advanced Payloads," Aerospace and Defense News.
[46] Ibid.
[47] "Fact Sheet: US Contributions to NATO Capabilities," US Mission to NATO, 8 July 2016, https://nato.usmission.gov/fact-sheet-u-s-contributions-to-nato-capabilities/.
[48] Ibid.
[49] David P. Watson and David H. Scheidt, "Autonomous Systems," 371.
[50] Ibid., 374-375.
[51] Ibid.
[52] Chairman of the DSB, *Summer Study on Autonomy*, 83-85.
[53] David P. Watson and David H. Scheidt, "Autonomous Systems," 374-375.
[54] Chairman of the DSB, *Summer Study on Autonomy*, 83-85.
[55] Ibid.
[56] Ibid., 1.
[57] Jose Carreno et al., "What's New About the AirSea Battle Concept," *Proceedings Magazine*, no. 136 (August 2010): 290.
[58] Chairman of the DSB, *Summer Study on Autonomy*, 1.
[59] Ibid., 6.
[60] "The Mercedes-Benz Future Bus," Daimler Auto Group, 15 January 2017, https://www.daimler.com/innovation/autonomous-driving/future-bus.html.
[61] Chairman of the DSB, *Summer Study on Autonomy*, 6.
[62] Rick Zhang, "Autonomous Mobility-on-Demand – A Solution for Sustainable Urban Personal Mobility," Stanford Energy Club, 7 April 2014, https://energyclub.stanford.edu/autonomous-mobility-on-demand-a-solution-for-sustainable-urban-personal-mobility/.
[63] Chairman of the DSB, *Summer Study on Autonomy*, 1.

[64] US Navy, *A Cooperative Strategy for 21st Century Seapower* (Washington, DC: Department of the Navy, 2015), 33.
[65] US Navy, *2015 Navy Program Guide* (Washington, DC: Department of the Navy, 2015), 70.
[66] Lt Col Erik C. Bowman, "ISR PED System in support of Global Strike in 2035," 18-19.
[67] Chairman of the DSB, *Summer Study on Autonomy*, 21-23.
[68] Lt Col Erik C. Bowman, "ISR PED System in support of Global Strike in 2035," 11.
[69] Chairman of the DSB, *Summer Study on Autonomy*, 1
[70] Ibid.
[71] Ibid.
[72] David P. Watson and David H. Scheidt, "Autonomous Systems," 368

Bibliography

Aerospace and Defense News. "Elbit Systems' Hermes 900: Equipped with Multiple Advanced Payloads." 6 February 2012. http://www.asdnews.com/news-40818/Elbit_Systems__Hermes_900:_Equipped_with_Multiple_Advanced_Payloads,_this_UAS_is_Leading_its_Class_in_Multi-Mission_Performance.htm.

Air Force, US. *2015 Program Element 0603742F: Combat Identification Technology Budget Item Justification Exhibit*. Washington, DC: Headquarters US Air Force, March 2014.

Air Force, US. *Global Vigilance, Global Reach, Global Power for America*. Washington, DC: Headquarters US Air Force, 2013.

Anderson, John. *Hypersonic and High-Temperature Gas Dynamics Second Edition*. Reston, VA: American Institute of Aeronautics and Astronautics, 2006.

Beason, Doug. *The E-Bomb: How America's Directed Energy Weapons Will Change The Way Future Wars Will Be Fought*. Cambridge, MA: Da Capo Press, 2005.

Bowman, Lt Col Erik C. "Intelligence, Surveillance, and Reconnaissance Processing, Exploitation, and Dissemination System in support of Global Strike in 2035." Master's thesis, Air War College, February 2012.

Capozzella, Lt Col Robert J. "High Power Microwaves on The Future Battlefield: Implications for US Defense." Master's thesis, Air War College, 17 February 2010.

Carreno, Jose et al. "What's New About the AirSea Battle Concept." *Proceedings Magazine*, no. 136 (August 2010): 290.

Chief Scientist, US Air Force. *Technology Horizons: A Vision for Air Force Science and Technology 2010-30*. Washington, DC: Office of the US Air Force Chief Scientist, September 2011.

Chiefs of Staff, Joint. *Joint Publication 3-14: Space Operations*. Washington, DC: Office of the Joint Chiefs of Staff, 2013.

Clarke, Richard A., and Robert K. Knake. *Cyber War*. New York, NY: Harper-Collins Publishers, 2010.

Curtis E. LeMay Center for Doctrine Development and Education. *Volume 1, Air Force Basic Doctrine*. 27 February 2015. https://doctrine.af.mil/dnv1vol1.htm.

Daimler Auto Group. "The Mercedes-Benz Future Bus." Accessed 15 January 2017. https://www.daimler.com/innovation/autonomous-driving/future-bus.html.

DeAngelis, Stephen F. “Artificial Intelligence: How Algorithms Make Systems Smart.” *Wired*. September 2014. https://www.wired.com/insights/2014/09/artificial-intelligence-algorithms-2/.
Deep-Mind Lab. “AlphaGo Games.” Accessed 21 January 2017. https://deepmind.com/research/alphago/.
Defense Science Board, Chairman. *Summer Study on Autonomy*. Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, June 2016.
Elbit Systems. “Hermes 900.” Accessed 19 February 2017. http://elbitsystems.com/product/hermes-900-5/.
Hall, J. Storrs. *Nanofuture:What’s Next for Nanotechnology*. Amherst, NY: Prometheus Books, 2005.
Hambling, David. *Swarm Troopers*. Charleston, SC: Archangel Ink, 2015.
Johnson, Kenneth F. “The Need For Speed: Hypersonic Aircraft And The Transformation Of Long Range Airpower.” Master’s thesis, School and Advanced Air and Space Studies, June 2005.
Joint Chiefs of Staff, Chairman. *Joint Operating Environment 2035.* Washington, DC: Office of the Joint Chiefs of Staff, 14 July 2016.
Kurzweil, Ray. *The Singularity Is Near*. New York, NY: Penguin Books, 2006.
Lindhom, Capt Garrison. “Intelligence Control and Evaluation of Teams (ICE-T).” Presentation. AFRL Aerospace Directorate, Wright Patterson AFB, OH, 24 August 2016.
McCarthy, John. “What is Artificial Intelligence: Basic Questions.” Standford.edu. 12 November 2007. http://www-formal.stanford.edu/jmc/whatisai/node1.html.
Navy, US. *2015 Navy Program Guide*. Washington, DC: Department of the Navy, 2015.
Navy, US. *A Cooperative Strategy for 21st Century Seapower*. Washington, DC: Department of the Navy, 2015.
Ramo, Joshua C. *Seventh Sense*. New York, NY: Little, Brown and Company, 2016.
Russell, Stuart J., and Peter Norvig. *Artificial Intelligence: A Modern Approach Third Edition*. Upper Saddle River, NJ: Prentice Hall, 2009.
US Mission to NATO. “Fact Sheet: US Contributions to NATO Capabilities.” 8 July 2016. https://nato.usmission.gov/fact-sheet-u-s-contributions-to-nato-capabilities/.
Watson, David P. and David H. Scheidt. “Autonomous Systems.” *Johns Hopkins APL Technical Digest* 26, no. 4 (2005): 368-376.
Williams, Brian G. *Predators: The CIA’s Drone War on al Qaeda*. Washington, DC: Potomac Books, 2013.
Zhang, Rick. “Autonomous Mobility-on-Demand – A Solution for Sustainable Urban Personal Mobility.” Stanford Energy Club. 7 April 2014. https://energyclub.stanford.edu/autonomous-mobility-on-demand-a-solution-for-sustainable-urban-personal-mobility/.