REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
04/30/2019	Master's of Military Studies	SEP 2018 - APR 2019

4. TITLE AND SUBTITLE

AMORPHOUS SWARMS:
ASYMMETRIC AUTONOMOUS AIRCRAFT AFFECTING ADVERSARY AIR DEFENSE DECISIONS

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Kowalski, Jordan, A Major, USMC

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

10. SPONSOR/MONITOR'S ACRONYM(S)
Dr Benjamin Jensen

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

SUAS Swarms provide an expanded reconnaissance and decoy capability against enemy IADS. Asymmetric SUAS swarms can be utilized to influence an IADS targeting and weapon employment in a peer and near-peer conventional conflict. SUAS swarms, equipped to mirror the RCS and flight characteristics of a known US air asset, will be a viable means to convince enemy radar operators at the tracking and targeting radar levels to activate for friendly targeting. These swarms require artificial intelligence advances to perform true autonomous coordination to achieve the deception effect while actively collecting on enemy systems.

15. SUBJECT TERMS

Swarm, drone, remotely piloted aircraft (RPA), integrated air defense system (IADS), artificial intelligence (AI), small unmanned aerial vehicle (SUAS), integrated air defense system (IADS)

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			USMC Command and Staff College
					19b. TELEPHONE NUMBER *(Include area code)*
Unclass	Unclass	Unclass	UU	25	(703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

AMORPHOUS SWARMS:
ASYMMETRIC AUTONOMOUS AIRCRAFT AFFECTING ADVERSARY AIR DEFENSE DECISIONS

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

AUTHOR:
Major Jordan Kowalski US Air Force

AY 18-19

Mentor ~~and Oral~~ Defense Committee Member: Dr Benjamin Jensen
Approved: _____
Date: 4/29/19

Oral Defense Committee Member: Nathan Packard, PhD
Approved: _____
Date: 4/29/2019

Executive Summary

Title: Amorphous Swarms: Asymmetric Autonomous Aircraft Affecting Adversary Air Defense Decisions

Author: Major Jordan Kowalski, US Air Force

Thesis: The threat presented by peer and near-peer A2AD systems affects every domain of warfare. The early warning and guidance radars for the A2AD integrated air defense system (IADS) alert the mainland forces of any imminent approach of hostile aircraft. Advances in small unmanned aerial system (SUAS) swarms, artificial intelligence (AI), and an increase in the functionality of larger remotely piloted aircraft (RPA) offer a means to affect the enemy's targeting cycle by deceiving the radars and presenting an unclear threat picture which would theoretically delay the employment of weapons while providing targeting data for United States (US) and allies. The US military should be able to utilize SUAS and larger RPA swarms, or asymmetric RPA swarms (ARS) to present and monitor enemy IADS radars with the purpose of delaying IADS engagement of friendly forces or making the enemy IADS engage less-valuable targets, exposing both radar and transporter erector launchers (TEL) for neutralization.

Discussion: Peer and near-peer adversaries have established extremely complex anti-access and area denial (A2AD) systems that seek to limit international actors from achieving strategic and tactical advantage near their claimed sovereign territory. SUAS and RPA in a swarm offer an opportunity to confuse the enemy's targeting cycle by providing misleading radar signatures that are able to mimic other aircraft and change their configuration to present a targeting dilemma for their IADS. There are contemporary efforts to create autonomous targeting drones that mimic specific aircraft radar cross sections (RCS), however the systems they mimic are already being replaced. Smaller, less-expensive aircraft with the ability to create multiple radar signatures could create doubt after reports of a specific type of aircraft within the early warning radar's range, only for the signature's characteristics change drastically. The enemy would be forced to spend time and energy investigating the potential threat rather than being able to react to their first indication. Each of the swarms would attempt to mimic another RCS, detect and report radar energy directed at the swarm, then change formation or flight characteristics to confuse enemy targeting. Current systems would require AI augmentations to react appropriately absent any input from an operator in a contested electromagnetic (EM) environment. The ARS AI should be able to change configuration to present multiple types of RCS as well as decide what, if any, maneuvers to make to react to both radar and kinetic fires.

Conclusion: Asymmetric RPA swarms would provide a significant resource and decision cycle drain on enemy IADS employment. The ARS would coordinate within the swarm to mimic the radar signatures of larger, more threatening aircraft in an attempt to elicit a response from acquisition and targeting radar systems. The ARS would detect and report radar sites and activity to targeting cells beyond radar acquisition range for neutralization. Should the adversary fire upon the ARS, the swarm would have options on how to react such as taking the hit, attempting to dodge, or reconfiguring its formation. In a future conflict with a peer or near-peer, having flexible options to degrade the enemy's operational decision cycle, even for a short while, will prove the difference between success and failure.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

Table of Contents

Preface

This concept paper is intended to inspire use of current and future small unmanned aerial systems swarms in penetrating and deceiving adversary integrated air defense systems. The scenarios, examples, and technologies explained are US military service branch agnostic and represent a means to deceive and defeat enemy systems.

.

General

A military's decision-making cycle requires both speed and clarity to be effective at all levels of war. The ultimate goal is to alter the decision landscape in such a way that an opposing force may make poor decisions, or delay a decision, based on inaccurate or false information. Each misstep or delay offers an opportunity for the opposing side to monitor, assess, and adjust their scheme of maneuver.

The difficulty in deceptive operations stems from successfully convincing the enemy that bad information is correct or that good information might not be accurate. Modern technology, specifically the multitude of potential sources of information, enables those with access to verify the accuracy of a given bit of information.

Artificial intelligence and machine learning play a part in corroborating information rapidly from numerous sources in order to determine what is true. Integrated sensors networks feed many US, peer, and near-peer homeland defense systems with strict rules of engagement (ROE) to employ lethal force.[1] The specific details and ROE of employment are classified, but the basics include a layered sensor network of radar and sonar systems to identify at long-range air and sea vehicles approaching sovereign territory. Aircraft or ship detection is then tracked and the sensor return's characteristics (size, speed, approach vector) can then be fed to shorter range sensor systems for tracking and if necessary, targeting. Once the target is identified within a certain probability as hostile, an approval authority gives the authorization to engage with some type of munition.

In terms of affecting a defensive system, such as an IADS, creating doubts about what might be on the horizon and whether or not to actively scan (radiate) for then engage a potential target can waste resources and expose radar sites and surface to air missiles (SAM) batteries to

long-range fires. Early warning radar (EWR) can scan for thousands of miles, which allows for ample time to observe and analyze a given radar signature but also time to induce doubt.[2] Defensive SAM munitions cost millions of dollars, making the decision to employ them weighted against the surety that the employment will indeed protect the homeland against a perceived threat.[3] A trained radar operator would likely be able to classify an unknown radar track as hostile then inform their reporting chain accordingly.[4] A nation's IADS must be accurate and employed with care to avoid wasting a high value missile or destroying civilian aircraft.[5] Any doubts as to the intentions and type of aircraft maneuvering within the detection range of IADS radar systems warrants an analytic response.

Purpose

The purpose of this future concept paper is to introduce the idea for developing a new type of IADS deceptive unmanned aerial system (UAS) amorphous swarm (IDUAS) to counter and degrade the enemy's decision cycle regarding the employment of an IADS. This paper will discuss the conceptual technology utilized to constitute the swarms, the AI needed to coordinate, and the supporting systems to make the swarms effective.

Historical Case Support

The 21st century's global dynamic allowed the rise of peer and near-peer threats to US dominance in the various spheres of influence presented in many international relations models. The revisionist powers identified in the NSS, namely China and Russia, have installed a significant series of deterrents and barriers around their claimed borders with their A2AD systems.[6] These systems in peer and near-peer territory typically make use of long range weaponry to deter competitive forces from entering the owner's territory.[7] These weapons are alerted to and cued by advanced detection systems such as EW radars as a part of an IADS. These EW radar systems are

able to detect and measure the speed and RCS of an aircraft or surface ship from a significant distance, allowing for analysis and weapon-target pairing for neutralization. An analogous example of a peer conflict is the Bekaa Valley War in 1982, specifically Operation Mole Cricket 19, between Israel and an alliance of Lebanon and Syria.[8] The Israeli Air Force (IAF) utilized remotely piloted vehicles (RPVs) coupled with an effective ISR reporting chain to deceive, target, and destroy the enemy's IADS. Though modern US attack aircraft reportedly have the superb radar mitigation technology, the limited number and high cost of each unit precludes a full scale penetration of a peer's IADS for strike without substantial and significant losses. Therefore, the US's strike aircraft could learn significant lesson as to how the IAF utilized RPVs during Mole Cricket.

The IAF's success in the 1982 conflict rose from hard lessons learned during the Arab-Israeli War of 1973. The Syrians and Egyptians used surprise and a Soviet IADS to take a heavy toll on the IAF during the opening days of the fighting; the IAF lost 14% of its initial aircraft sorties.[9] New tactical SAMS, such as the SA-6 and SA-7, complicated IAF attempts to establish air superiority over the theater SAMS such as the SA-2 and SA-3. Israel did not employ a typical pre-emptive strike due to mounting international pressure and a lack of target intelligence prior to the Egypt-Syria attacks.[10] The SAMS, combined with enemy aircraft and ADA led to rapid changes in how the IAF employed against their adversaries to keep from total loss in the air. The IAF's new tactics relied on deceiving enemy IADS nodes with manned aerial feints and baiting SAM sites into revealing themselves for follow on attacks.[11] This was still risky for the aircraft involved which the IAF was determined to change in future conflicts.

The strategic lessons from the 1973 Arab-Israeli War (also called the Yom Kippur War) reinforced the IAF's strategic impetus to disable an enemy's IADS to establish air superiority

quickly. Attacks by the Palestinian Liberation Organization (PLO) with support from Syria staged from Lebanon escalated tensions into the Bekaa Valley Conflict. Syrian SAMS were moved into Lebanon to protect their assets attacking Israeli interests along the border, pushing Israel to action.[12] The Israelis utilized RPVs to locate and track mobile SAMS and monitored the radar systems targeting those same RPVs for analysis.[13] The Soviet radars employed were able to track many targets, but were unable to discriminate the small ISR RPVs from attack aircraft and unknowingly exposed themselves to Israeli anti-radar munitions. The RPVs directly contributed to the first four steps of an air targeting cycle and allowed the IAF to eliminate all 19 of the Syrian SAMs in the Bekaa Valley.[14] The use of RPVs to scout and decoy the IADS proved viciously effective and removed the IADS threat from the Israeli border rapidly.

The use of RPVs to scout and spoof enemy IADS was novel at the time and made more effective by poor employment by the Syrian forces in the Bekaa Valley.[15] US air planners can take some salient lessons from how the IAF employed relatively cheap but effective remotely piloted aircraft (RPA; contemporary parlance for RPV) to target SAMS without risk to manned pilots and aircraft. Current RPA are comparatively inexpensive with respect to modern fighter and bomber aircraft, but still cost tens of millions of dollars.[16] The targeting systems US RPA contain would be viable for finding, fixing, tracking, targeting, and when necessary engaging enemy IADS, but they would need to be well inside the SAM missile engagement zone (MEZ) to begin the targeting process. If each missile in a revisionist IADS is comparable in cost to a Patriot Missile used by the US, an RPA shoot-down is still cost effective for the defender.[17] Additionally, US medium-altitude, long-endurance, tactical (MALET) RPA maneuver slower and have a significantly different radar signature than manned fighter/bomber aircraft, allowing an observant enemy radar technician to prioritize targets toward the more expensive and lethal manned aircraft.

These facts, combined with the need to unravel the layers of an A2AD IADS, calls for a strategy like the IAF used in Operation Mole Cricket. The US should develop and implement an RPA system to spoof enemy A2 EW radar systems, accumulate and retransmit radar data for targeting, and ensure system is capable of acting in a signal-denied environment.

Operation Mole Cricket demonstrated the viability of inexpensive RPA to act as spotters and decoys against enemy IADS. Since the 1982 Arab-Israeli War, IADS technology has improved which theoretically allows well-trained crews to identify different aircraft signatures at greater range. The increased accuracy of IADS radars combined with faster means of communication within the decision channels of modern military formations could make an IADS kill-chain significantly shorter. To hinder the command's decision-making process, new RPA may be implemented to distract, deceive, and still target enemy IADS. The RPA must be inexpensive enough to be mass-produced quickly and allow for significant losses to achieve a given objective. There are systems currently in development which fit part of this description such as the Gremlin which is being developed by DARPA to act as expendable but recoverable RPA.[18] The mission or payload the Gremlin will carry is unspecified. Another system developed by Raytheon, the Miniature Air-Launched Decoy (MALD), acts in a similar manner to the Gremlin with respect to delivery from airborne assets ahead of a strike package.[19] The MALD intends to spoof enemy IADS into targeting them by mimicking other aircraft radar signatures which allows strike assets to neutralize the radar or SAMS as they reveal themselves.[20] Each of these systems provides a modern example of how RPA could affect an IADS targeting and decision matrix like in Mole Cricket.

One of the major successes of Operation Mole Cricket is utilizing inexpensive RPA to provide real-time targeting updates for counter SAM attacks. Mole Cricket RPA were small and

lacked the ability to organically strike their targets, but could provide targeting data or even laser terminal guidance to friendly munitions.[21] This changed the dynamic with respect to anti-IADS air campaigns as RPA were not considered for tactical combat. RPA were, and to some degree still are, categorized as "drones" which operate autonomously to carry out a specific set of tasks or fly a certain pattern for aerial target practice. Bekaa Valley showed that with the correct integration of need, technology, and planning, RPA could be an effective warfighting platform. Modern MALET aircraft, such as the MQ-9 or RQ-170, drew heavy inspiration from the IAF's use of RPA for target tracking and marking. The eventual addition of munitions capable of striking the targets located by the RPA was the logical next step.

An advantage modern A2AD systems have over the Syrian forces is standoff. Due to the close proximity of Bekaa Valley to Israeli bases, the RPA and IAF manned aircraft were only dealing with relatively small MEZ distances, 14 nautical miles in the case of the SA-6, which meant a relatively short delay from launch to target acquisition for tracking.[22] Systems such as the MALD, Gremlin, or Coyote all provide means to launch into IADS EW radar ranges, but lack the proximity of rapid target acquisition. The tyranny of distance presented by revisionist IADS, particularly China, means that future systems seeking to mimic Mole Cricket success must be capable of being launched from beyond a manned threat MEZ. One of the final considerations is payload compared to survivability. The IAF was willing to use their inexpensive RPA to stimulate the air defenses while using adequate real-time video to target the SAM launchers.[23] Contemporary real-time situational awareness tools require free use of the electromagnetic spectrum to fully realize their potential. Conflicts with peers will likely have communications severely degraded.

Operation Mole Cricket was a decisive victory for the IAF and airpower theory. The IAF's use of RPA to spoof Syrian SAMS into tracking limited value targets revealed the SAM locations and provided real-time tracking of the SAM launchers for targeting. The coordination of the ISR RPA, central IAF control, and the IAF strike aircraft allowed for the rapid destruction of the Syrian SAM threat in the region, leading to IAF air superiority. Mole Cricket demonstrates RPA as a vector for deceiving enemy radar and IADS systems while providing targeting data against those same systems. However, more must be done to improve anti-IADS RPA efforts when combatting peer or near-peer adversaries. Current RPA do not have the proximity to their area of operations as the IAF did in Bekaa Valley, necessitating the development of extremely long range RPA to enact a similar mission. Finally, Mole Cricket's signal management was a non-factor as there were no reported instances of Syrian signal interference with IAF assets, and wars against peers will have severely degraded signals across all spectrums, making use of targeting data difficult. However, Operation Mole Cricket offers definitive proof that RPA are a feasible asset in gaining aerial access.

Time Horizons, Assumptions, and Risks

The timeline to develop the new IDUAS is uncertain and depends on the ability to develop several technologies simultaneously. Current UAS swarm developed by the US Defense Advanced Research Projects Agency (DARPA) demonstrate the ability to launch and recover their low-cost gremlins from a large cargo aircraft, presently a C-130, demonstrates the ability to launch and recovery SUAS swarms.[24] DARPA's Gremlins prove airborne launched SUAS swarms are possible, and adapting their employment to different aircraft and outfitting them with different payloads is feasible within a few years.[25] The risk associated with the current delivery system, or similar large cargo aircraft deliveries, is their inherent vulnerability to anti-aircraft threats due to a

large RCS, relatively low airspeed, and lack of maneuverability. Given that EWRs can see, track, and classify large aircraft from hundreds of miles away, a different delivery platform would be required. The gremlin swarms are anticipated to be adapted to different delivery methods with an implied assumption that they will eventually be adapted to a wing-mounted launch system, but could (and should) be adapted to internal munitions employment storage.[26] Creating an adaptive delivery system for other-than-cargo aircraft should be feasible within the next five years based on existing platform developments like the Coyote from Raytheon.[27] These swarms would also require upgrades to their propulsion to ensure they can match the speed of the aircraft they're attempting to mimic.

Current SUAS, like the coyote, are propeller driven, which gives off a different RCS than a jet-powered aircraft. The assumption is that technology will advance to allow IDUAS-like swarms to operate at much faster speeds and for much longer distances to allow. Additionally uncertain is the ability for AI to contribute to the employment of the IDUAS. Swarming right now relies on multiple aircraft being controlled via a single controlling station or having each aircraft act within the confines of a pre-programmed set of flight parameters.[28] For the technology to work as intended, swarming technology would require advancement to have swarm operate within its given parameters with minimal human input. The risk in swarm AI failing to advance is IDUAS failing to elicit the desired reaction from an adversary's IADS due to the swarm failing to behave in a manner that convinces an IADS operator there is a threatening aircraft within their detection range. The risk inherent in waiting to develop and perfect the swarm AI technology is that conflict between the US and a peer adversary with advanced A2AD capabilities arrives before such technology is ready, putting US lives at risk.

Description of the Military Problem

Enemy sensing systems, such as radars in an IADS, coupled with long-range precision fires from advanced SAMs make maneuvering through and to the enemy's territory incredibly dangerous. EWRs are able to scan and track for thousands of miles and in a contemporary A2AD environment, able to strike ship, aircraft, or even ballistic missiles from hundreds of miles away.[29] As previously discussed, SAMs are expensive and making an adversary fire one or several missiles at targets that are not of significant value can make an enemy question if they should employ more. The ever expanding reach, combined with the ability to see and sense well beyond the horizon truly limits the US's ability to arrive at an adversary's homeland should conflict arise.

There is an opportunity to counter the rising A2AD threat by making enemy IADS and sensing equipment detect false radar signatures presented by advanced swarms combined with AI. Using relatively inexpensive assets able to adapt and change their presentation to the enemy should create confusion within the sensing reporting chain and afford opportunities for US and allied systems to identify, track, locate, and if necessary eliminate adversary SAM and radar sites to allow follow-on forces freedom of maneuver.

Central Idea

UAS similar to Coyotes or Gremlins would be deployed in small swarms from aircraft, ground launched mechanisms, or ships with the intent to stimulate an enemy's IADS or sensing equipment and present a signature that mimics that of a given desired aircraft. The purpose behind the deception is to convince the enemy that a false aircraft is within their IADS detection range. This induces confusion by forcing the enemy to choose one of several courses of action to US benefit. The first is corroborate the EWR indications with some other real-time or near-real-time source. Since the IDUAS is programmed to mimic and present a signature of a given aircraft in

radar and electronic emissions, multi-source correlation should confirm the IDUAS is what its signature is presenting while causing the enemy to radiate from multiple sites to confirm. If the enemy is close enough to utilize visual confirmation to identify the swarm, it has likely successfully delayed IADS action which should allow follow on aircraft to penetrate the airspace. While presenting a potential threat and the enemy IADS is attempting to discern the aircrafts nature and intent, a second function the IDUAS would serve is to utilize sensing equipment of its own to locate, track, and retransmit the location of any radar sites to a relay craft for future or immediate prosecution. Finally, should the enemy chose to engage the low-cost swarm with expensive missiles, imposing both monetary cost and wasting the missile on a less-than-threatening target, the missile launches would immediately expose TEL locations for targeting and counter-battery fire to eliminate the threat.

The swarms' AI would be able to automatically adjust its flight profile depending on the type of mission assigned. Should the swarm be launched for simple probing of the IADS, the swarm could, at the first sign of an acquisition radar, reconfigure itself to present a different radar signature target entirely or even disperse to make several smaller targets. This would have the benefit of potentially encouraging enemy IADS operators to doubt their equipment or force the enemy to waste resources (aircraft sorties, satellite re-tasking, repositioning naval surface vessels) to visually confirm targets because their electronic sensing lost the target or the information presented was considered unreliable. A secondary effect to scrambling assets to visually confirm a potential threat also creates alert fatigue, whereby constantly sitting on alert for enemy action severely reduces readiness and combat effectiveness.[30] Again, depending on when and how the IDUAS detected radar signals, the swarm's mission parameters would dictate its behavior and it

would act appropriately and independently assuming a degraded control signal in an A2AD environment.

An insight from three wargames conducted against peer adversaries are that SUAS employed against an IADS are generally ignored unless they have demonstrated a tangible threat to the enemy. Most Red interactions with limited Coyote swarms were to note their presence and carry on with their activities. Red swarm disruption in the wargames focused on attempting to jam signals between the SUAS aircraft and their controlling station based on current generation limitations discussed earlier.[31] Therefore, autonomy and resilience will help mission success through survivability and a small measure of independence. Finally, if the signature presented is not a threat, Red IADS are unlikely to spend munitions attempting to neutralize them.

Application and Integration of Military Functions

The IDUAS would be employed during the early stages of an air campaign or during specific air missions to protect air assets or degrade enemy IADS. The IDUAS would be launched and recovered from different sites in order to confuse enemy tracking, sometimes launched from air and recovered by ship or launched by land and recovered by an aircraft. A mission from an air launched platform would likely proceed as follows:

> *In calendar year 2030, Avenger 44 flight, a pair of MQ-31s modeled after the General Atomics Predator-C design, is scheduled to perform an IADS ISR mission over a large body of water near a US peer adversary.[32] Avenger 44 flight each carry two Mimic IDUAS swarms which are programmed with a mission to emulate a flight of F-16s near the enemy's target acquisition radar. Simultaneously, a fleet of Naval super destroyers, armed with hypersonic rail cannons, are maneuvered to within their engagement range but just beyond the*

anti-surface missile range. Avenger 44 flight launches and within 40 miles of the target acquisition radar deploys their Mimic swarms and maneuver to just inside the Mimic's transmission range to protect itself and pass the data accumulated and transmitted by the Mimic flights. The Mimics coordinate internally and create a formation that, according to radar, maneuver and read as a two flights of two F-162. The faux F-16s are equipped with radar detection and direction finding equipment to relay any target acquisition radars that attempt to "paint" them. The Mimic flights fly within the suspected enemy missile engagement zone (MEZ), and detect several different radar signatures attempting to gain a target lock. Mimics then transmit the radar's data to Avenger 44 which passes the data to the Super Destroyer. The Super Destroyer directs one Mimic flight to remain on station and attempt to show defensive maneuvering, while the other is directed to disperse and reform in different locations to confuse enemy targeting. The swarms perform as directed and when the enemy fires on them, one mimic sub-swarm is "killed" by the enemy's missile while the other three sub-swarms disperse and return to their launcher while the Super Destroyer uses its rail-gun to destroy the radars and TELs. The manned fighter and cargo aircraft that have been standing by then are able to press into the gap in the IADS flanked by more Mimics providing radar screens and false targets to protect the larger aircraft.

In all aspects of the fictitious scenario above, the swarms are performing ISR, signal retransmission, deception, and targeting for follow-on fires and aerial maneuver.

Necessary Capabilities

Swarm technology would need to evolve to allow the individual parts of the group of entities (in this case SUAS) to coordinate their positioning and activities within the group without the express input from a remote user. Current swarms are programmed, managed, and flown through a centralized input terminal requiring human input to monitor and correct the SUAS flights.[33] In an A2AD environment, line-of-sight (LOS) communications by radio or data burst can be assumed to be degraded to the point of ineffectiveness, requiring a large degree of autonomy on the swarm's behalf. The IDUAS's AI could be programmed to react to certain stimuli (radio calls, radar, and jammers) in specific ways to present a realistic flight profile of a given spoofed aircraft. The swarm AI would subsequently need to be robust enough to manage operations of several individual aircraft and change the aircraft's flight formation in order to meet mission parameters. The AI, upon recognizing pre-determined stimuli, would need to know to transmit all relevant data to an extra-swarm source, or if the launch platform is another RPA, a remote part of the swarm.

The transmission of data in an EM degraded or denied environment would require utilizing different communications means. Possibilities include a light based, directional data burst toward an expected receiving source or possibly using quantum communications to securely transmit the information. Both signaling technologies are currently in development. Barring future communications technology, a directed data-burst transmission to a receiver is likely the most practical means.

To fully mimic a bevy of aircraft signatures, SUAS technology would need to move away from the lighter, slower, propeller driven RPA of the current generation and change to a faster, jet propulsion system if the signature is to be genuine enough to induce confusion. The engines would

also require a similar duration to the aircraft they mimicked, which could change depending on what the mission called for. Larger swarms could mimic larger aircraft, which could necessitate the endurance to match. However, if the swarms were considered disposable, fuel efficiency would be a luxury versus a necessity.

Finally, if IDUAS recovery was desired, a number of options to divert the swarms to and from. Examples like the proposed MQ-31 of an RPA launching the IDUAS swarms could incorporate the launch platform into the swarm as a relay or "parent" aircraft directing the movements of the sub-swarms. Other options should be explored with respect to land-based or sea-based recovery of the assets. Alternative airborne launch platforms might be from an aerial refueling or command and control aircraft, but given how far removed most high-value airborne assets (HVAA) from MEZ threats, the swarms would require engines and endurance to reach their target areas.

Spatial and Temporal Dimensions

As mentioned, a new and different delivery vehicle would enable short range swarms the ability to reach the target provided the swarms could not fly the entire way on their own. Alternatively, the swarms could be created to increase their range and endurance requiring no intermediary launch and recovery asset. In an arena where aircraft are able to launch within the MEZ, such as a hypothetical scenario against a rogue state where the US already has bases nearby, the IDUAS could be launched from air, land, or sea. Given the proximity to the enemy in that scenario, a launch from another aircraft would delay visual identification of the swarms from the ground.

In a longer distance scenario where our aircraft or ships would need to traverse for long distances under the watch of an enemy's EWR, the swarms do not have the mission endurance to

reach the enemy's mainland on their own. In this case, having alternative launch and land sites in-theater would boost their on-station capability as well as reducing the amount of assets needed to launch the IDUAS. The longer an IDUAS could remain in a given IADS, the longer it would risk discovery. However, loitering in the IADS provides ample opportunity for the swarms to perform ISR on IADS locations and capabilities. The DARPA Gremlin aircraft are currently projected to be viable through 20 missions so extremely hazardous missions could be assigned to aircraft at the end of their lifecycle to preserve newer capabilities while still penetrating dangerous airspace.[34]

Launching from within a MEZ increases on-station time, removes the problem of penetrating the outer IADS layers while immediately allowing ISR collection to start in a relatively short amount of time. The previously discussed wargames conducted against robust and complex IADS demonstrated that assets launched within the MEZ and acquisition radars were able to locate and maneuver successfully against the enemy systems in rapid order. The closer the aircraft's launches were to a given IADS system, the sooner US forces were able to locate, target, and neutralize that threat. All maneuvers from beyond the MEZ were subsequently tracked and engaged a much longer ranges. Though more likely to miss, enemy MEZ capabilities would keep manned and HVAA assets beyond a useful range. Therefore, if possible, establishing launch sites within the IADS belts or even within a MEZ will provide a positional advantage to US conflicts in the future.

Conclusion

In a high-end conventional fight against peers and near-peers, the United States must take every opportunity to degrade and delay opposing military structures from effective decision making. With A2AD constructs that extend hundreds of miles from a coastal or land border, the US will have to work hard penetrating the defenses just to bring traditional military might to bear.

Air provides a fast, efficient, and lethal means to rapidly engage enemy forces but still incurs significant risk to human operators and expensive assets. IDUAS swarms provide a means to confuse enemy targeting, waste resources and time confirming targets, expend long-range weapons against a cost-inefficient target, and expose vital targeting radars and weapons platforms. The potential low-cost and adaptive nature of the swarm allows them to be expendable but immensely effective in an anti-IADS campaign. Current technology allows for a similar but simplified solution to the IADS problem set, so further development is necessary for the concept to remain viable against future threats. However the risk of failing to maintain air superiority in support of friendly maritime and land forces demands that every avenue of advantage be fully explored.

[1] NATO, "NATO Integrated Air and Missile Defence," (NATO.int, 7 Jun 2018,) https://www.nato.int/cps/en/natohq/topics_8206.htm.
[2] Katherine Owens, "The Air Force upgrades its missile early warning systems," (DefenseSystems.com, 24 Apr, 2017, https://defensesystems.com/articles/2017/04/24/earlywarningradar.aspx)
[3] Derek Hawkins, "A U.S. 'ally' Fired a $3 Million Patriot Missile at a $200 Drone. Spoiler: The Missile Won." (The Washington Post. March 17, 2017)
[4] Air Force Instruction (AFI) 11-2E-3V3, *E-3 Operations Procedures*, Headquarters Air Combat Command, 2 March 2016), 46.
[5] Netherlands Government Press, "MH17: The Netherlands and Australia hold Russia responsible," (Netherlands Government Website, 25 May 2018, https://www.government.nl/latest/news/2018/05/25/mh17-the-netherlands-and-australia-hold-russia-responsible)
[6] Ben Jackman, "Understanding the Anti-Access and Area Denial Threat: An Army Perspective," (US Army Command and General Staff College, Ft Leavenworth, KS, 4 January 2015), 11
[7] Ibid, 14
[8] Rebecca Grant, "The Bekaa Valley War," (Air Force Magazine, June 2002), 58.
[9] Bradley D. Darling, "Establishing Operational Access: Insights from the Past for the Future," (Air University Press, Maxwell AFB, AL. June 2014.) 62
[10] Ibid, 63
[11] Ibid, 64
[12] Rebecca Grant, "The Bekaa Valley War," (Air Force Magazine, June 2002), 59.
[13] Matthew M. Hurley, "The BEKAA Valley Air Batle, June 1982: Lessons Mislearned?" (Airpower Journal, Winter 1989.) 4.
[14] Rebecca Grant, "The Bekaa Valley War," (Air Force Magazine, June 2002), 61
[15] Matthew M. Hurley, "The BEKAA Valley Air Batle, June 1982: Lessons Mislearned?" (Airpower Journal, Winter 1989.) 4.
[16] US Air Force Fact Sheets, "MQ-9 Reaper," (USAF Public Affairs, September 23, 2015.)
[17] Derek Hawkins, "A U.S. 'ally' Fired a $3 Million Patriot Missile at a $200 Drone. Spoiler: The Missile Won." (The Washington Post. March 17, 2017)
[18] Scott Wierzbanowski, "Gremlins," Defense Advanced Projects Agency Program Information, Accessed 14 December 2018.
[19] Raytheon Corp. "MALD Decoy: Disrupting Enemy Air Defense Systems," Raytheon Products & Services Listing, Waltham MA, Accessed 15 Dec 2018.
[20] Ibid
[21] Matthew M. Hurley, "The BEKAA Valley Air Batle, June 1982: Lessons Mislearned?" (Airpower Journal, Winter 1989.) 4.

[22] Air Force Techniques, Tactics, and Procedures (AFTTP) 3-2.6, ***JFIRE*** *Multi-Service Tactics, Techniques, and Procedures for Joint Application of Firepower,* Air Land Sea Application Center, January 2016, 117.

[23] David Rodman, "Unmanned Aerial Vehicles In The Service Of The Israel Air Force: "They Will Soar On Wings Like Eagles," Middle East Review of International Affairs, Vol. 14, No. 3 September 2010, 77.

[24] Defense Advanced Research Projects Agency (DARPA), "Gremlins on Track for Demonstration Flights in 2019," (DARPA Outreach, 9 May 2018. https://www.darpa.mil/news-events/2018-05-09)
[25] ibid
[26] ibid
[27] Raytheon Corp. "Coyote UAS, One System: Multiple Missions," (Raytheon Products & Services Listing, Waltham MA, Accessed 16 Dec 2018.) https://www.raytheon.com/capabilities/products/coyote
[28]Jason Kehe, "Drone Swarms as you know them are just an Illusion- for now," (Wired.com, 14 August, 2018. https://www.wired.com/story/drone-swarms-are-an-illusion-for-now/)
[29]Alicia Sanders-Zakre, "China Advances Ballistic Missile Defense," (Arms Control Today, 1 September 2017, https://www.armscontrol.org/act/2017-09/news-briefs/china-advances-ballistic-missile-defense)
[30] Jan Goldman, *Intelligence Warning Terminology*¸ Joint Military Intelligence College, Washington DC, October 2001.
[31] Jason Kehe, "Drone Swarms as you know them are just an Illusion- for now," (Wired.com, 14 August, 2018. https://www.wired.com/story/drone-swarms-are-an-illusion-for-now/)
[32] General Atomics Fact Sheet, "Predator C Avenger," (General Atomics Aeronautical Systems Inc, 19 Feb 2015)
[33] Jason Kehe, "Drone Swarms as you know them are just an Illusion- for now," (Wired.com, 14 August, 2018. https://www.wired.com/story/drone-swarms-are-an-illusion-for-now/)
[34] Defense Advanced Research Projects Agency (DARPA), "Gremlins on Track for Demonstration Flights in 2019," (DARPA Outreach, 9 May 2018. https://www.darpa.mil/news-events/2018-05-09)

Bibliography

Air Force Instruction (AFI) 11-2E-3V3, *E-3 Operations Procedures*, Headquarters Air Combat Command, 2 March 2016.

Air Force Techniques, Tactics, and Procedures (AFTTP) 3-2.6, ***JFIRE*** *Multi-Service Tactics, Techniques, and Procedures for Joint Application of Firepower*, Air Land Sea Application (ALSA) Center, January 2016.

Darling, Bradley D. "Establishing Operational Access: Insights from the Past for the Future," Air University Press, Maxwell AFB, AL. June 2014.

Defense Advanced Research Projects Agency (DARPA), "Gremlins on Track for Demonstration Flights in 2019," DARPA Outreach, 9 May 2018. https://www.darpa.mil/news-events/2018-05-09

General Atomics Fact Sheet, "Predator C Avenger," General Atomics Aeronautical Systems Inc, 19 Feb 2015

Goldman, Jan, *Intelligence Warning Terminology*¸ Joint Military Intelligence College, Washington DC, October 2001.

Grant, Rebecca, "The Bekaa Valley War," Air Force Magazine, June 2002.

Hawkins, Derek. "A U.S. 'ally' Fired a $3 Million Patriot Missile at a $200 Drone. Spoiler: The Missile Won." The Washington Post. March 17, 2017. https://www.washingtonpost.com/news/morning-mix/wp/2017/03/17/a-u-s-ally-fired-a-3-million-patriot-missile-at-a-200-drone-spoiler-the-missile-won/?noredirect=on&utm_term=.c6fe257f9101

Holt, Thaddeus, *The Deceivers: Allied Military Deception in the Second World War*. Simon and Schuster, May 11, 2010.

Hurley, Matthew M. "The BEKAA Valley Air Batle, June 1982: Lessons Mislearned?" Airpower Journal, Winter 1989.

Jackman, Ben, "Understanding the Anti-Access and Area Denial Threat: An Army Perspective," US Army Command and General Staff College, Ft Leavenworth, KS, 4 January 2015

Kehe, Jason, "Drone Swarms as you know them are just an Illusion- for now," Wired.com, 14 August, 2018. https://www.wired.com/story/drone-swarms-are-an-illusion-for-now/

Kreis, John F. "Unmanned Aircraft in Israeli Air Operations." *Air Power History* 37, no. 4 (1990): 46-50. http://www.jstor.org/stable/26271146.

Milstein, Uri, "Operation Mole Cricket 19: 34 Years Later, The IAF's Most Decisive Victory Remains The Standard," Jarusalem Press, Israel, 18 July, 2016. https://www.jpost.com/Magazine/Operation-Mole-Cricket-19-456909

Netherland Government Press, "MH17: The Netherlands and Australia hold Russia responsible," Netherlands Government Website, 25 May 2018, https://www.government.nl/latest/news/2018/05/25/mh17-the-netherlands-and-australia-hold-russia-responsible

North Atlantic Treaty Organization (NATO), "NATO Integrated Air and Missile Defence," NATO.int, 7 Jun 2018, https://www.nato.int/cps/en/natohq/topics_8206.htm, Accessed 14 March 2019

Owens, Katherine, "The Air Force upgrades its missile early warning systems," DefenseSystems.com, 24 Apr, 2017, https://defensesystems.com/articles/2017/04/24/earlywarningradar.aspx

Raytheon Corp. "MALD Decoy: Disrupting Enemy Air Defense Systems," Raytheon Products & Services Listing, Waltham MA, Accessed 15 Dec 2018. https://www.raytheon.com/capabilities/products/mald

Raytheon Corp. "Coyote UAS, One System: Multiple Missions," Raytheon Products & Services Listing, Waltham MA, Accessed 16 Dec 2018. https://www.raytheon.com/capabilities/products/coyote

Rodman, David, "Unmanned Aerial Vehicles In The Service Of The Israel Air Force: "They Will Soar On Wings Like Eagles," Middle East Review of International Affairs, Vol. 14, No. 3 September 2010.

Sanders-Zakre, Alicia, "China Advances Ballistic Missile Defense," Arms Control Today, 1 September 2017, https://www.armscontrol.org/act/2017-09/news-briefs/china-advances-ballistic-missile-defense.

The White House. *The National Security Strategy of the United States of America.* Washington, DC, Dec 2017. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

US Air Force Fact Sheets, "MQ-9 Reaper," USAF Public Affairs, September 23, 2015. https://www.af.mil/About-Us/Fact-Sheets/

Wierzbanowski, Scott, "Gremlins," Defense Advanced Projects Agency Program Information, Accessed 14 December 2018. https://www.darpa.mil/program/gremlins