REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
15-05-2015	FINAL	

4. TITLE AND SUBTITLE

Operational Protection from Unmanned Aerial Systems

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Daniel A. Boutros

Paper Advisor (if Any): **Prof. Albion Bergstrom, CAPT Hans Sholley**

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

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

12. DISTRIBUTION / AVAILABILITY STATEMENT

For Example: Distribution Statement A: Approved for public release; Distribution is unlimited. Reference: DOD Directive 5230.24

13. SUPPLEMENTARY NOTES A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

The widespread proliferation of Unmanned Aerial Systems (UAS) among both state and non-state actors is cause for concern to U.S. Operational Commanders. No longer does the U.S. have a monopoly on UAS operations. Nearly 90 countries now operate some type of UAS capability and, with increasingly affordable and available technology, that trend is increasing at an alarming rate. This paper evaluates the current and anticipated future threat posed by adversary UAS to U.S. forces, both in the form of system capabilities and methods of employment. It also addresses present counter UAS capabilities and recommends ways and means to provide better operational protection. Throughout the paper, the term 'UAS' encompasses all types of unmanned aircraft and is used synonymously with the terms Unmanned Aerial Vehicle (UAV), Remotely Piloted Aircraft (RPA), and drone.

15. SUBJECT TERMS

Operational Protection, Unmanned Aerial Systems, UAS, Counter-UAS, UAV, Counter-UAV

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Chairman, JMO Dept
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		22	19b. TELEPHONE NUMBER *(include area code)* 401-841-3556

Standard Form 298 (Rev. 8-98)

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
15 MAY 2015		**00-00-2015 to 00-00-2015**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Operational Protection from Unmanned Aerial Systems	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Joint Military Operations Department,,Naval War College, 686 Cushing Rd.,,Newport,,RI,02841**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The widespread proliferation of Unmanned Aerial Systems (UAS) among both state and non-state actors is cause for concern to U.S. Operational Commanders. No longer does the U.S. have a monopoly on UAS operations. Nearly 90 countries now operate some type of UAS capability and, with increasingly affordable and available technology, that trend is increasing at an alarming rate. This paper evaluates the current and anticipated future threat posed by adversary UAS to U.S. forces, both in the form of system capabilities and methods of employment. It also addresses present counter UAS capabilities and recommends ways and means to provide better operational protection. Throughout the paper, the term ???UAS??? encompasses all types of unmanned aircraft and is used synonymously with the terms Unmanned Aerial Vehicle (UAV), Remotely Piloted Aircraft (RPA), and drone.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a REPORT	b ABSTRACT	c THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**23**	

NAVAL WAR COLLEGE
Newport, R.I.

OPERATIONAL PROTECTION FROM UNMANNED AERIAL SYSTEMS

by

Daniel A. Boutros

LCDR, U.S. Navy

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College of the Department of the Navy.

Signature: _____

15 May 2015

Contents

Abstract

The widespread proliferation of Unmanned Aerial Systems (UAS) among both state and non-state actors is cause for concern to U.S. Operational Commanders. No longer does the U.S. have a monopoly on UAS operations. Nearly 90 countries now operate some type of UAS capability and, with increasingly affordable and available technology, that trend is increasing at an alarming rate. This paper evaluates the current and anticipated future threat posed by adversary UAS to U.S. forces, both in the form of system capabilities and methods of employment. It also addresses present counter UAS capabilities and recommends ways and means to provide better operational protection. Throughout the paper, the term 'UAS' encompasses all types of unmanned aircraft and is used synonymously with the terms Unmanned Aerial Vehicle (UAV), Remotely Piloted Aircraft (RPA), and drone.

INTRODUCTION

As of 2010, 40 countries possessed Unmanned Aerial System (UAS) technology.[1] By the end of 2013 that number had grown to almost 90, and though most are low-technology Intelligence, Surveillance, and Reconnaissance (ISR) platforms, over 30 nations have some type of armed UAS program.[2] These numbers do not include non-state actors, which often obtain UAS from sponsoring states or commercial venues. Joint Publication (JP) 3-01 identifies friendly assets that an adversary may attack during a campaign using unmanned aircraft and which must be protected under a commander's counterair plan, including: air defense sites, command and control (C2) elements, communication nodes, air facilities, logistics centers, and critical infrastructure.[3] But due to their small size and unique flight envelopes, many UAS are difficult to detect, identify, track, and engage with the current joint air defense system.[4] The widespread proliferation of UAS has exposed a critical vulnerability in the protection function of operational commanders, requiring additional joint efforts that include intelligence, electronic warfare (EW), cyber warfare, and fires.

On the bright side, unmanned systems are not invincible. Operational Commanders can utilize current joint force capabilities to neutralize the threat or reduce the risk to within acceptable levels. These include active and passive methods of defense and kinetic or non-kinetic fires. Testing is also underway to

[1] P.W. Singer, "Will Foreign Drones One Day Attack the U.S.?," *Newsweek*, 25 February 2010. http://www.newsweek.com/will-foreign-drones-one-day-attack-us-75331.
[2] Michael C. Horowitz and Matthew Fuhrmann, "Droning On: Explaining the Proliferation of Unmanned Aerial Vehicles" (research paper, University of Pennsylvania and Texas A&M University, 2014), 2.
[3] Chairman, U.S. Joint Chiefs of Staff, *Countering Air and Missile Threats*, final coordination, Joint Publication (JP) 3-01 (Washington DC: CJCS, 23 March 2012), I-7.
[4] Ibid.

develop new technologies and operational concepts that combine systems and improve C2 structures to make the fight against enemy UAS more effective.

UAS PROLIFERATION

To understand both the proliferation of and threat posed by UAS, it is necessary to identify those qualities that make them appealing. The most obvious is that it reduces the risk to pilots. For every aircraft shot down, that country loses a highly trained pilot, often with years of flying experience that is difficult to replace. Although using an unmanned aircraft does not take the human out of the equation, it does allow him or her to walk away from the control console if something were to go wrong.[5] UAS also provide for better ISR than manned aircraft because of their longer on-station time. Some of the more advanced systems can loiter for up to twenty hours conducting ISR - significantly longer than manned aircraft.[6] Furthermore, UAS deliver similar capabilities to manned aircraft at a fraction of the cost. This makes UAS especially attractive to countries that wish to establish a form of air power without the expensive buildup for an air force or cruise missile programs. Unmanned aircraft can be pieced together from commercially available parts for less than $1,000, with militarized versions costing as little as $10,000.[7] UAS technology is affordable, available, and relatively easy to operate. The increased capabilities at reduced risk and cost make UAS highly desirable.

To date, the proliferation of more advanced systems has been limited to nations that already have the industry and infrastructure to support them. Countries possessing

[5] Michael C. Horowitz and Matthew Fuhrmann, "Droning On: Explaining the Proliferation of Unmanned Aerial Vehicles" (research paper, University of Pennsylvania and Texas A&M University, 2014), 10.
[6] Ibid., 15.
[7] P.W. Singer, "Will Foreign Drones One Day Attack the U.S.?," *Newsweek*, 25 February 2010. http://www.newsweek.com/will-foreign-drones-one-day-attack-us-75331.

advanced systems capable of long-range precision strike include the U.S., United Kingdom, Israel, and China.[8] Other equally sophisticated UAS are operated by nations such as Russia, India, Iran, Pakistan, Turkey, the United Arab Emirates, and most Western European nations.[9] Such systems require complex ground control facilities and logistical lines of support. As a result, they are less likely to find their way into the hands of non-state actors.

Low technology systems, however, are prime for proliferation to any interested party. Because of their relatively simple command and control requirements and lower costs, many nations and non-state actors are opting to acquire them from more technologically advanced allies rather than develop their own. China and Iran are among the major proliferators of UAS. In fact, some experts believe that by 2025 China will be responsible for the production of over half the world's UAS.[10] Furthermore, Iranian systems like the long-range, low technology Ababil have been supplied to nations such as Syria and Sudan, as well as terrorist and extremists groups like Hezbollah, Hamas, and the Islamic State of Iraq and Syria/Sham (ISIS).[11] In fact, Hezbollah's current UAS inventory is estimated at over 200 aircraft, causing a great deal of concern among Israeli military commanders.[12]

---

[8] Michael C. Horowitz and Matthew Fuhrmann, "Droning On: Explaining the Proliferation of Unmanned Aerial Vehicles" (research paper, University of Pennsylvania and Texas A&M University, 2014), 4.
[9] Lynn E. Davis et al., *Armed and Dangerous? UAVs and U.S. Security*, RAND Report RR-449-RC (Santa Monica, CA: RAND, 2014), 9.
[10] Michael S. Chase et al., *Emerging Trends in China's Development of Unmanned Systems*, RAND Report RR-990-OSD (Santa Monica, CA: RAND, 2015), 7.
[11] Wim Zwijnenburg, "Drone-tocracy? Mapping the Proliferation of Unmanned Systems," *Sustainable Security*, 8 October 2014, accessed 6 April 2015, http://sustainablesecurity.org/2014/10/08/drone-tocracy-mapping-the-proliferation-of-unmanned-systems/.
[12] Ibid.

UAS CAPABILITIES AND VULNERABILITIES

> *Unmanned Aircraft are being developed with more technologically advanced systems and capabilities. They can duplicate some of the capabilities of manned aircraft for both surveillance/reconnaissance and attack missions. They can be small enough and/or slow enough to elude detection by standard early warning sensor systems and could pose a formidable threat to friendly forces.*[13]
>
> - JP 3-01, Countering Air and Missile Threats

Advanced UAS are capable of carrying large payloads great distances. In keeping with the Missile Technology Control Regime, an international agreement intended to limit cruise missile and UAS proliferation, those payloads are considered to be at least 500 kg, with UAS ranges of at least 300 km.[14] U.S. Predator and Global Hawk UAS, as well as the Chinese Pterodactyl and Soaring Dragon counterparts, and the Iranian Ababil fall into this category.[15] Advanced UAS can be either armed or unarmed, with payloads capable of ISR, communications relay, over-the-horizon (OTH) target acquisition and tracking, and precision strike. This allows an adversary to achieve operational or even strategic reach to shape the battlefield and directly affect centers of gravity.

Shorter range, tactical, small, or micro UAS may not have the reach or payload capacity of more advanced systems, but can affect a campaign in equally serious ways. Because of their small size and almost nonexistent heat signatures, they are able to evade detection, and provide an adversary with more freedom of action. The fact that they can

---

[13] Chairman, U.S. Joint Chiefs of Staff, *Countering Air and Missile Threats*, final coordination, Joint Publication (JP) 3-01 (Washington DC: CJCS, 23 March 2012), V-6.
[14] Lynn E. Davis et al., *Armed and Dangerous? UAVs and U.S. Security*, RAND Report RR-449-RC (Santa Monica, CA: RAND, 2014), 23.
[15] P.W. Singer, "Will Foreign Drones One Day Attack the U.S.?," *Newsweek*, 25 February 2010. http://www.newsweek.com/will-foreign-drones-one-day-attack-us-75331.

be launched from within U.S. air defense zones and fly to their targets in less time than it takes for a coordinated response enables an enemy to effectively balance space, time, and force.[16] For the first time in decades, an enemy may be able to fly aircraft in close proximity to U.S. ground forces and thereby challenge U.S. air superiority.[17] Small UAS can perform short-range ISR, be outfitted with explosive charges or chemical and biological agents for aerial dispersion, or simply fly over troops to produce a desired reaction to be exploited. Given the devastating effects that Improvised Explosive Devices (IEDs) have had over the last decade of warfare in Iraq and Afghanistan, a mobile, airborne version would take the problem to an entirely new level. In this way many believe small UAS pose the more significant threat - one for which the U.S. is not prepared.

> *The proliferation of low cost, tactical unmanned aerial systems demand we think about this potential threat now… We must understand the threat these systems present to our joint force and develop the tactics, techniques, and procedures to counter the problem.*[18]
>
> - General James N. Mattis, former Commander, U.S. Joint Forces Command

Developing technologies do not paint a pleasant picture for the counter-UAS problem. Some UAS, such as the Hummingbird developed by AeroVironment, are meant to mimic flying objects found in nature, further complicating detection and

[16] Laurent Beaudoin et al., *Potential Threats of UAS Swarms and the Countermeasure's Need*, European Conference on Information Warfare and Security (ECIW) (Tallin, Estonia: 2011), 24.
[17] Matthew Neuenswander, "Wargaming the Enemy Unmanned Aircraft System Threat," *Fires* PB644-12, no. 6 (November-December 2012): 59.
[18] F. Patrick Filbert and Darryl Johnson, "Joint Counter Low, Slow, Small Unmanned Aircraft Systems Test," *Fires* PB644-14, no. 4 (July-August 2014): 21.

identification challenges.[19] Additionally, advancements in automation are making systems less dependent on their data links with ground control stations. Entire mission and navigation profiles can now be preprogrammed into a UAS prior to launch. UAS are also becoming smarter, with the ability to make decisions and react in response to their environment. Real-time coordination with other autonomous UAS will soon allow swarms of small, unmanned aircraft to conduct simultaneous attacks on a target from multiple directions.[20]

Thankfully, UAS have significant vulnerabilities that can be exploited. In June 2014, Hamas attempted to use an Iranian Ababil over Israel, but it was successfully shot down by a Patriot missile.[21] In the early stages of the Global War on Terrorism, the U.S. discovered that air superiority was a prerequisite for its use of drones, as the more advanced systems used by the U.S. tended to be larger and susceptible to traditional Integrated Air Defense Systems (IADS). The Global Hawk, for instance, has a wingspan of over 130 feet, larger than a Boeing 737 commercial airliner, and is easily picked up by ground-based radars.[22] For smaller systems, however, more cunning approaches are required.

An evaluation of unmanned systems from a technical perspective reveals they are vulnerable to non-kinetic outside influence in three distinct areas: their link to a ground

[19] Christina Hernandez Sherwood, "Everyday Drones" *Government Technology* 25, no. 8 (August 2012): 15.
[20] Laurent Beaudoin et al., *Potential Threats of UAS Swarms and the Countermeasure's Need*, European Conference on Information Warfare and Security (ECIW) (Tallin, Estonia: 2011), 24.
[21] Wim Zwijnenburg, "Drone-tocracy? Mapping the Proliferation of Unmanned Systems," *Sustainable Security*, 8 October 2014, accessed 6 April 2015, http://sustainablesecurity.org/2014/10/08/drone-tocracy-mapping-the-proliferation-of-unmanned-systems/.
[22] Eric Beidel, "Uncertainty, Challenges Mark Future for Military's Unpiloted Aircraft," *National Defense* 95, no. 683 (October 2010): 28.

control station, the ground control station itself, and the aircraft's various sensors.[23] The link between an aircraft and its ground control station is vulnerable to hacking. It was reported in both 2008 and 2009 that Iraqi insurgents successfully hacked into U.S. Reaper drones, causing them to crash.[24] Ground control stations, as with all networked computers, are susceptible to viruses. In September 2011, the ground control stations at Creech Air Force Base in Nevada were infected by the Keylogging virus, temporarily grounded the entire UAS fleet.[25] The various onboard sensors can be manipulated in many ways. High-intensity light directed at an optical sensor can jam it and effectively blind the UAS. GPS receivers can be 'spoofed,' which consists of transmitting a stronger, but false GPS signal to a receiver, resulting in inaccurate navigation. At the request of the Department of Homeland Security, a team from the University of Texas's Radionavigation Laboratory successfully spoofed a UAS at the White Sands Missile Range in the summer of 2012.[26] Finally, influencing the local magnetic field can have adverse effects on both onboard hard drives and sensors that require magnetic orientation to operate correctly.[27] By properly understanding UAS subsystems, exploiting weaknesses is limited only by one's ingenuity.

[23] Kim Hartmann and Christoph Steup, *The Vulnerability of UAVs to Cyber Attacks – An Approach to the Risk Assessment* (Tallinn: NATO CCD COE Publications, 2013), 6.
[24] Michael C. Horowitz and Matthew Fuhrmann, "Droning On: Explaining the Proliferation of Unmanned Aerial Vehicles" (research paper, University of Pennsylvania and Texas A&M University, 2014), 12.
[25] Kim Hartmann and Christoph Steup, *The Vulnerability of UAVs to Cyber Attacks – An Approach to the Risk Assessment* (Tallinn: NATO CCD COE Publications, 2013), 1.
[26] "U.S. Confirms UAVs Vulnerable to Electronic Jamming, Capture," *Geo-Strategy Direct*, 11 July 2012, accessed 8 April 2015, EBSCO.
[27] Kim Hartmann and Christoph Steup, *The Vulnerability of UAVs to Cyber Attacks – An Approach to the Risk Assessment* (Tallinn: NATO CCD COE Publications, 2013), 15.

CURRENT PROTECTIVE MEASURES

JP 3-01, Countering Air and Missile Threats, charges Joint Force Commanders with the responsibility of creating a joint operation plan that includes air and missile defense. As part of the command and control structure for this task, an Area Air Defense Commander (AADC) and Airspace Control Authority (ACA) are designated, who in turn develop area air defense and airspace control plans to provide comprehensive counterair operations.[28] The Joint Force Air Component Commander (JFACC) normally takes on the roles of both AADC and ACA. Counterair operations can be either offensive (OCA) or defensive (DCA), and attempt to provide the required level of air superiority and protection to achieve a commander's operational objectives.[29]

"The preferred method of countering air and missile threats is to destroy or disrupt them prior to launch using OCA operations conducted over enemy territory."[30] To make such efforts successful, intelligence on the enemy air order of battle includes aircraft inventory, capabilities, and locations. This then allows for coordinated targeting of those assets to shape the battlefield and make air superiority easier to achieve.

DCA brings together multiple sensors, communications, command and control, and weapons systems into an IADS.[31] To provide an adequate level of protection, U.S. IADS follow a defense in depth concept. As inbound threats are detected, they are identified and tracked, then defeated as far from the area of operations as possible. This may mean engaging it with fighter aircraft or surface to air missiles. If these efforts are

[28] Chairman, U.S. Joint Chiefs of Staff, *Countering Air and Missile Threats*, final coordination, Joint Publication (JP) 3-01 (Washington DC: CJCS, 23 March 2012), II-3.
[29] Ibid., III-1.
[30] Ibid., IV-1.
[31] Ibid., V-3.

not enough, point defenses are established around critical forces or installations. Finally, self-defense measures can be taken from individual units affected by the threat.[32]

As stated earlier, advanced UAS can be detected, identified, and tracked by current IADS. Furthermore, these systems can be engaged and easily shot down by current fighter aircraft.[33] Current protective measures, therefore, are only adequate to protect against larger, more advanced UAS.

PROTECTION SHORTFALLS

Joint Publication 3-01 highlights the difficulties involved with countering the small UAS threat, but provides little practical guidance to overcome those difficulties. Current IADS are inadequate to protect against small, tactical UAS. Current radar systems are unable to detect small UAS, and IADS cannot identify, track, or engage what they cannot see. Even if a small UAS were detected, fighters would have difficulty engaging it due to low altitudes and slow speeds. Additionally, since a small UAS can have a very short flight time to its target, the timeline from detection to engagement is compressed. The decision to engage a threat must be made quickly, and at lower levels than currently employed. What is most likely to happen is that the soldier on the ground will be the first to detect an enemy UAS. This means the outer two layers of defense, namely area defense and point defense, have failed and all that remains is unit or individual self-defense. If the soldier is fortunate enough to detect a UAS while it is

[32] Chairman, U.S. Joint Chiefs of Staff, *Countering Air and Missile Threats*, final coordination, Joint Publication (JP) 3-01 (Washington DC: CJCS, 23 March 2012), V-11-12.
[33] Lynn E. Davis et al., *Armed and Dangerous? UAVs and U.S. Security*, RAND Report RR-449-RC (Santa Monica, CA: RAND, 2014), 3.

enroute to some other target, there exists no way for him to upload what he knows to a common operational picture in time for effective action to be taken.[34]

To make up for this critical vulnerability and fill the gap in the operational function of protection, the U.S. needs enhanced detection capabilities, EW, C2, personnel training, and engagement systems to defeat enemy UAS either kinetically or non-kinetically.

COUNTER ARGUMENT

Some might argue that small, low technology UAS do not pose a serious threat to U.S. forces because the weak state and non-state actors expected to use them have cheaper and more assured means of carrying out the same effects. UAS attack methods can be broken down into three basic categories: direct, indirect, or aerial dispersal.[35] For each of these, cheaper means are available for carrying out such attacks. A direct attack consists of using a weapon to directly impact a target. Cheaper alternatives for this mode of attack include mortars, snipers, rocket-propelled grenades, IEDs, suicide bombers, explosive-laden vehicles, etc., often with significantly greater payloads and explosive potential than a UAS. Indirect attacks are ones used to produce a response, to be exploited by some follow-on event, such as a diversion. Other available means of indirect attack include bomb threats, planting false intelligence, and feigned ground attacks. Even aerial dispersion attacks can be more efficiently conducted. Despite the relatively affordable price of smaller, low technology UAS, using rockets, mortars,

[34] Matthew Neuenswander, "Wargaming the Enemy Unmanned Aircraft System Threat," *Fires* PB644-12, no. 6 (November-December 2012): 63.
[35] Brian A. Jackson et al., *Evaluating Novel Threats to the Homeland – Unmanned Aerial Vehicles and Cruise Missiles*, RAND Report MG-626-DTRA (Santa Monica, CA: RAND, 2008), 16.

helium balloons, or even releasing an agent from the roof of a building would accomplish the same effects at a fraction of the cost.[36]

Additionally, since UAS are more complex systems than alternative attack methods, there is more opportunity for things to go wrong. The U.S.'s own General Roger A. Brady, U.S. Air Force (retired), who last served as Commander of U.S. Air Forces in Europe, voiced his dissatisfaction with UAS command signals, "a million miracles happen along optical links and it ends up in Las Vegas. I'm not even confident we've mapped that whole thing."[37] He went on to explain that the entire process could be defeated with commercially available off-the-shelf equipment. GPS jammers, for instance, are available on the Internet for approximately $1000.[38] And in 2008, the U.S. intercepted Al-Qaeda documents that described measures to counter a Predator UAS.[39] With the knowledge of such vulnerabilities, and the availability of cheaper, more reliable methods of attack, it is highly unlikely that weak states and non-state actors would invest their funds in UAS capabilities.

REBUTTAL

Though adversaries can achieve similar effects with less exotic means, the advantage that a UAS offers, and perhaps the reason why some groups are already using them despite the monetary costs and operational risks, is that it enables more freedom of action. A UAS provides operational reach into previously impenetrable areas and allows

[36] Brian A. Jackson et al., *Evaluating Novel Threats to the Homeland – Unmanned Aerial Vehicles and Cruise Missiles*, RAND Report MG-626-DTRA (Santa Monica, CA: RAND, 2008), 17-18.
[37] Eric Beidel, "Uncertainty, Challenges Mark Future for Military's Unpiloted Aircraft," *National Defense* 95, no. 683 (October 2010): 30.
[38] "U.S. Confirms UAVs Vulnerable to Electronic Jamming, Capture," *Geo-Strategy Direct*, 11 July 2012, accessed 8 April 2015, EBSCO.
[39] Eric Beidel, "Uncertainty, Challenges Mark Future for Military's Unpiloted Aircraft," *National Defense* 95, no. 683 (October 2010): 30.

an asymmetric means of challenging U.S. air superiority. With their ability to evade detection and reach their targets before a coordinated response can be enacted, small, tactical UAS provide a viable solution to U.S. defense perimeters.[40] The adversary can also better protect his forces by controlling UAS from safe distances, and reduce self-imposed attrition resulting from suicide tactics.

The psychological effects an enemy UAS can have on U.S. forces and civilian populations should not be underestimated. The very presence of an adversarial UAS in a commander's area of operations may feed directly into an enemy's propaganda campaign, highlighting the gap in U.S. protection, and creating distrust and insecurity between the U.S., a host nation, and its people. Furthermore, troop morale is negatively affected by the presence of enemy UAS. Even if a UAS does not directly attack troops on the ground, those troops have no way of knowing if the UAS is simply conducting ISR or is there to enable OTH targeting. Either way, the threat of attack is enough to distract forces from their primary objectives. During a series of joint UAS defense exercises hosted by the U.S. Army Training and Doctrine Command in 2008 and 2009, ground commanders saw persistent enemy UAS as 'prohibitive interference,' alluding to the criteria required for air superiority as defined in JP 1-02.[41]

Finally, the claim that fragile state and non-state actors will not use UAS because they have more cost-effective and reliable means of attack is refuted by real events. Hezbollah has been building an inventory of UAS since 2006, and has launched UAS attacks on Israel multiple times. Syria used UAS in battles near Aleppo and Damascus in

[40] Brian A. Jackson et al., *Evaluating Novel Threats to the Homeland – Unmanned Aerial Vehicles and Cruise Missiles*, RAND Report MG-626-DTRA (Santa Monica, CA: RAND, 2008), 71.
[41] Matthew Neuenswander, "Wargaming the Enemy Unmanned Aircraft System Threat," *Fires* PB644-12, no. 6 (November-December 2012): 59-60.

ISR and targeting roles, as did Sudan in operations against rebel groups. Finally, ISIS released two videos in 2014 taken from their own surveillance UAS of armored convoys in Fallujah, Iraq and a military base near Raqqa, Syria.[42] The threat from small, tactical drones is a very real one for which the U.S. is unprepared.

CONCLUSIONS

The widespread proliferation of UAS technology is cause for concern among U.S. operational commanders. Today, nearly 90 countries and multiple non-state groups use UAS. Although advanced systems are capable of ISR and precision strike over long distances with considerable payload capacity, they are also vulnerable to current IADS. The proliferation of advanced systems is limited to those nations mature enough to support the complex infrastructure required. Despite the fact that small UAS lack the range and payload capacity of advanced models, they constitute the more dangerous threat. With their small size and slow flight profiles, they can avoid detection and are difficult to engage. Proliferation of these UAS is accelerated by their affordability and the capabilities they provide to weak adversaries – balancing space, time, and force to achieve operational reach and increased freedom of action. These systems can be used for ISR or OTH targeting, in direct attacks against forces, installations, and population centers, or in indirect ways to promote a specific response. The UAS capability affords asymmetric means to challenge U.S. air superiority and defensive perimeters.

Current air defenses are inadequate to protect against the small UAS threat, but UAS technology does have vulnerabilities that operational commanders can exploit. The

[42] Wim Zwijnenburg, "Drone-tocracy? Mapping the Proliferation of Unmanned Systems," *Sustainable Security*, 8 October 2014, accessed 6 April 2015, http://sustainablesecurity.org/2014/10/08/drone-tocracy-mapping-the-proliferation-of-unmanned-systems/.

link with its ground control station can be intercepted or jammed. GPS receivers can be spoofed, other onboard sensors can be blinded or manipulated, and onboard computers can be damaged by magnetic fields. Taking advantage of these weaknesses while employing joint efforts to enhance current IADS is the key to protecting friendly forces and populations from the emerging threat.

RECOMMENDATIONS

The best active defense against the enemy small UAS threat is an integrated, joint endeavor, which combines elements of intelligence, EW, cyber warfare, and fires. Joint intelligence efforts need to start during Phase 0 (Shape), before a conflict begins. This includes an evaluation of UAS proliferation within the theater of operations to determine which nations or groups possess UAS capabilities and at what level. The Joint Intelligence Preparation of the Operational Environment (JIPOE) should also establish an enemy UAS order of battle, identifying numbers, capabilities, ground control stations, and launch sites.[43] Finally, technical intelligence on foreign UAS design should be used to illuminate vulnerabilities in specific systems.[44]

Current air defense sensors must be upgraded to detect, identify, and track small, slow UAS. They must also be portable to protect convoys and forces operating away from their home installations. Other EW measures should be coupled with cyber capabilities to degrade, jam, or disorient the various UAS optical, navigational, and magnetic sensors. As point defenses, for instance, magnetic force generators coupled

[43] Matthew Neuenswander, "Wargaming the Enemy Unmanned Aircraft System Threat," *Fires* PB644-12, no. 6 (November-December 2012): 60.
[44] Brian A. Jackson et al., *Evaluating Novel Threats to the Homeland – Unmanned Aerial Vehicles and Cruise Missiles*, RAND Report MG-626-DTRA (Santa Monica, CA: RAND, 2008), xvii.

with GPS spoofing emitters can be employed around critical areas to defeat a UAS's ability to navigate.

Offensively, cyber warfare and fires can be employed individually or in unison to achieve either kinetic or non-kinetic effects. Based on the JIPOE, UAS threats should be included on the Joint Integrated Prioritized Targets List. Offensive Counterair (OCA) can then target them as operational fires designed to shape the battlefield.[45] Point defense cyber operations should be utilized to hack the command link between a UAS and its ground control station, even to the point of taking control of the aircraft if possible. For fleets or swarms of UAS, infecting the ground control stations with viruses could defeat multiple aircraft at once. Finally, surface to air missiles should be developed that can detect, track, and engage small UASs for kinetic effects.

Several civilian and military research and development teams are working on systems and methods to counter the low, slow, small UAS threat. One such company, Syracuse Research Corp, Inc. (SRC), specializes in artillery-detecting radars. When the U.S. Army put out a requirement for smaller, portable, and more capable radars to detect mortars, SRC came through with a cylindrical radar small enough to mount to a moving vehicle that can detect flying mortars in 360 degrees.[46] SRC then took their invention to the next level, making it capable of distinguishing birds and UAS, and incorporated EW systems previously used to disable IEDs. The combined system is capable of detecting, tracking, identifying, and defeating enemy UAS, either through kinetic or non-kinetic

[45] Matthew Neuenswander, "Wargaming the Enemy Unmanned Aircraft System Threat," *Fires* PB644-12, no. 6 (November-December 2012): 60.
[46] Dave Tobin, "SRC in Cicero Meets Army's Challenge to Save Lives with Anti-mortar Radar," *Syracuse.com,* 3 May 2010, accessed 16 April 2015, http://www.syracuse.com/news/index.ssf/2010/05/innovation_drives_surging_war.html.

means.[47] The kinetic effects are provided by the Switchblade UAS, a small, tube-launched UAS equipped with an explosive warhead, which is launched against an incoming enemy UAS. The system underwent testing at Pt. Mugu in August 2014 as part of BLACK DART, a joint counter-UAS exercise.[48] Such a system provides remarkable self-defense along with limited point defense capability, but does little in the way of area defense.

In an attempt to address the larger area defense issue, the U.S. Army's Fires Center of Excellence (FCOE) was assigned the lead in developing a counter UAS concept of operations.[49] It took over this responsibility from the Joint UAS Center of Excellence, which was disestablished in 2012.[50] Efforts by the Army's FCOE were joined by the U.S. Army Armaments Research, Development, and Engineering Center (ARDEC), as well as the Navy's Office of Strategic Systems Programs. The concept of operations calls for integrating sensors and weapon systems from multiple platforms and domains to detect, track, identify, and engage small UAS. In 2013 the concept was proven using Navy fire control radars to detect, track, and identify a UAS. Targeting information was then transmitted to a separate weapon platform on land, which defeated the threat.[51] Another joint effort, the Joint Counter Low, Slow, Small UAS Joint Test, was established in August 2012. The joint test aimed to develop and test the required C2

[47] SRC, Inc., "Counter-UAS Systems," accessed 16 April 2015, http://www.srcinc.com/what-we-do/ew/counter-uas.aspx?referrer=radar.
[48] Colin Clark, "New Weapons Spell Death for Drones; The Countermeasure Dance," *Breaking Defense*, 13 October 2014, http://breakingdefense.com/2014/10/new-weapons-spell-death-for-drones-the-countermeasure-dance/.
[49] Singh Bhavanjot and Eric Kowal, "Picatinny Counters Unmanned Aircraft System Threats," *Army.mil,* 7 January 2014, accessed 18 April 2015, http://www.army.mil/article/117902/picatinny_counters_unmanned_system_threats/.
[50] F. Patrick Filbert and Darryl Johnson, "Joint Counter Low, Slow, Small Unmanned Aircraft Systems Test," *Fires* PB644-14, no. 4 (July-August 2014): 22.
[51] Singh Bhavanjot and Eric Kowal, "Picatinny Counters Unmanned Aircraft System Threats," *Army.mil,* 7 January 2014, accessed 18 April 2015, http://www.army.mil/article/117902/picatinny_counters_unmanned_system_threats/.

architecture, with an emphasis on cross-domain intelligence sharing and improving the timely flow of information to an AADC. The focus of the joint test was not on creating new weapon systems, but on changing the processes used and incorporating more of the already existing sensors and weapon platforms within the joint force to increase capabilities.[52]

Although such development and testing of systems and processes is much needed, the protection they promise to the operational commander is still years away from being implemented. The threat is here now. It is up to each commander to mitigate that threat to acceptable levels by innovatively integrating the intelligence, EW, cyber, and fires capabilities currently at their disposal.

[52] F. Patrick Filbert and Darryl Johnson, "Joint Counter Low, Slow, Small Unmanned Aircraft Systems Test," *Fires* PB644-14, no. 4 (July-August 2014): 21.

Selected Bibliography

Beaudoin, Laurent, Antoine Gademer, Loica Avanthey, Vincent Germain, and Vincent Vittori. *Potential Threats of UAS Swarms and the Countermeasure's Need*. European Conference on Information Warfare and Security (ECIW). Tallin, Estonia: 2011.

Beidel, Eric. "Uncertainty, Challenges Mark Future for Military's Unpiloted Aircraft." *National Defense* 95, no. 683 (October 2010): 28-31.

Bhavanjot, Singh, and Eric Kowal. "Picatinny Counters Unmanned Aircraft System Threats." *Army.mil,* 7 January 2014. Accessed 18 April 2015. http://www.army.mil/article/117902/picatinny_counters_unmanned_system_threats/.

Chase, Michael S., Kristen A. Gunness, Lyle J. Morris, Samuel K. Berkowitz, and Benjamin S. Purser III. *Emerging Trends in China's Development of Unmanned Systems*. RAND Report RR-990-OSD. Santa Monica, CA: RAND, 2015.

Clark, Colin. "New Weapons Spell Death for Drones; The Countermeasure Dance." *Breaking Defense*, 13 Oct 2014. http://breakingdefense.com/2014/10/new-weapons-spell-death-for-drones-the-countermeasure-dance/.

Davis, Lynn E., Michael J. McNerney, James Chow, Thomas Hamilton, Sarah Harting, and Daniel Byman. *Armed and Dangerous? UAVs and U.S. Security*. RAND Report RR-449-RC. Santa Monica, CA: RAND, 2014.

Filbert, F. Patrick, and Darryl Johnson. "Joint Counter Low, Slow, Small Unmanned Aircraft Systems Test." *Fires* PB644-14, no. 4 (July-August 2014): 21-22.

Hartmann, Kim, and Christoph Steup. *The Vulnerability of UAVs to Cyber Attacks – An Approach to the Risk Assessment*. Tallinn: NATO CCD COE Publications, 2013.

Horowitz, Michael C. and Matthew Fuhrmann. "Droning On: Explaining the Proliferation of Unmanned Aerial Vehicles." Research paper, University of Pennsylvania and Texas A&M University, 2014.

Jackson, Brian A., David R. Frelinger, Michael J. Lostumbo, and Robert W. Button. *Evaluating Novel Threats to the Homeland – Unmanned Aerial Vehicles and Cruise Missiles.* RAND Report MG-626-DTRA. Santa Monica, CA: RAND, 2008.

Neuenswander, Matthew. "Wargaming the Enemy Unmanned Aircraft System Threat." *Fires* PB644-12, no. 6 (November-December 2012): 58-63.

Sherwood, Christina Hernandez. "Everyday Drones." *Government Technology* 25, no. 8 (August 2012): 11-17.

Singer, P.W. "Will Foreign Drones One Day Attack the U.S.?" *Newsweek*, 25 February, 2010. http://www.newsweek.com/will-foreign-drones-one-day-attack-us-75331.

SRC, Inc. "Counter-UAS Systems." Accessed 16 April 2015. http://www.srcinc.com/what-we-do/ew/counter-uas.aspx?referrer=radar.

Tobin, Dave. "SRC in Cicero Meets Army's Challenge to Save Lives with Anti-mortar Radar." *Syracuse.com,* 3 May 2010. Accessed 16 April 2015. http://www.syracuse.com/news/index.ssf/2010/05/innovation_drives_surging_war.html.

"U.S. Confirms UAVs Vulnerable to Electronic Jamming, Capture." *Geo-Strategy Direct*, 11 July 2012. Accessed 8 April 2015. EBSCO.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Countering Air and Missile Threats*. Final coordination. Joint Publication (JP) 3-01. Washington DC: CJCS, 23 March 2012.

Zwijnenburg, Wim. "Drone-tocracy? Mapping the Proliferation of Unmanned Systems." *Sustainable Security*, 8 October 2014. Accessed 6 April 2015. http://sustainablesecurity.org/2014/10/08/drone-tocracy-mapping-the-proliferation-of-unmanned-systems/.