SANDIA REPORT

SAND2015-6365
Unlimited Release

UAS Detection, Classification, and Neutralization: Market Survey 2015

Gabriel C. Birch, John C. Griffin, and Matthew K. Erdman

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Approved for public release; further dissemination unlimited.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online ordering: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2015-6365
Unlimited Release

UAS Detection, Classification, and Neutralization: Market Survey 2015

Gabriel C. Birch
Sandia National Laboratories
gcbirch@sandia.gov

John C. Griffin
Sandia National Laboratories
johgrif@sandia.gov

Matthew K. Erdman
Sandia National Laboratories
mkerdma@sandia.gov

Abstract

The purpose of this document is to briefly frame the challenges of detecting low, slow, and small (LSS) unmanned aerial systems (UAS). The conclusion drawn from internal discussions and external reports is the following; detection of LSS UAS is a challenging problem that cannot be achieved with a single detection modality for all potential targets. Classification of LSS UAS, especially classification in the presence of background clutter (e.g., urban environment) or other non-threating targets (e.g., birds), is under-explored. Though information of available technologies is sparse, many of the existing options for UAS detection appear to be in their infancy (when compared to more established ground-based air defense systems for larger and/or faster threats). Companies currently providing or developing technologies to combat the UAS safety and security problem are certainly worth investigating, however, no company has provided the statistical evidence necessary to support robust detection, identification, and/or neutralization of LSS UAS targets.

The results of a market survey are included that highlights potential commercial entities that could contribute some technology that assists in the detection, classification, and neutralization of a LSS UAS. This survey found no clear and obvious commercial solution, though recommendations are given for further investigation of several potential systems.

Contents

Appendix

Figures

Tables

1 Introduction

Detection of low, slow, and small (LSS) unmanned aerial systems (UAS) is quickly becoming an important capability for the maintenance of security. Consumer grade LSS UASs are becoming increasingly complex, and represent a diverse new threat which must be addressed by physical security systems of the future. This report surveys the existing landscape of technological solutions developed, or currently in development, to address the safety and security risks posed by LSS UASs.

Critical to the information gathered in this report is the North Atlantic Treaty Organization (NATO) Industrial Advisory Group Study SG-170, "The Engagement of Low, Slow and Small Aerial targets by GBAD (ground based aerial defense)." That document is the result of a 10 year study including analysis of LSS UAS engagement, which consists of detection, classification, and neutralization. The study specifically addresses the current and near-future threat spectrum, applicable sensors, potential neutralization techniques (called effectors), integration into existing GBAD architecture, and the existing gaps in security technology. The conclusions of the NATO report, most recently updated in July of 2013, states the following:

- Urgent action is necessary if the operational risks from these platforms are to be minimized and it requires the application of some innovative tactics and technologies to effectively counter these threats.
- No sensor type alone is able to provide sufficient tracking and identification capability to offer a reliable and effective defense against the LSS threat.
- To provide a satisfactory performance, the use of an adequate mix of sensors will be crucial.
- In light of the gaps at the effector and sensor level, it is proposed that a further study should be conducted to examine the optimum sensor/effector mix to counter the LSS evolving threat.

These statements are significant when considered in today's climate, where a near-term solution is desired for national security and civilian safety.

This document draws from and, to a certain extent, mirrors the efforts put forth by the NATO study, but we more specifically take a snapshot of the existing market technologies (both commercial and government sponsored) that can be integrated into or serve as a standalone counter UAS defense system. To give proper context, section 2 defines the LSS UAS target and presents various commercial examples, each of which provides a unique challenge to detection and identification. The high level detection modalities are discussed in section 3, including their positive and negative attributes when applied to LSS UAS. Section 4 discusses types of effectors and mitigation systems that may address some aspect of the LSS UAS threat. A major NATO report on LSS UAS engagement is summarized in section 5, and the recommendations of this NATO study are discussed. Section 6 and section 7 presents the results of the market survey for detection/identification and neutralization systems, respectively. Recommendations based on this survey are given in section 8.

2 LSS UAS Threat

The UAS market has grown substantially in the last 10 years, and the future looks bright with the NIAG report citing a projected 30,000 UASs used in the United States in the next decade. Hobbyist and military grade fixed wing UASs have been in use for years, but the substantial growth in popularity is largely attributed to advancements in rotary-blade UASs. These multi-blade systems typically are simple to control, have the ability to hover, and are cost effective, all of which contribute to a reduced barrier to entry for both civilian and military use. Less popular are the aerostat, balloon, or blimp aircraft. Regardless of the flight mechanism, all UAS types present their own set of challenges to safety and security,

2.1 Categorization

In order to categorize UASs for security purposes, the NIAG report defines them based on their mass and the typical capabilities that are associated with each class, as shown in table 1. Class I includes anything under 150 kg, while class II extends to the larger types between 150 and 600 kg. This upper class is, for now, generally restricted to military aircraft.

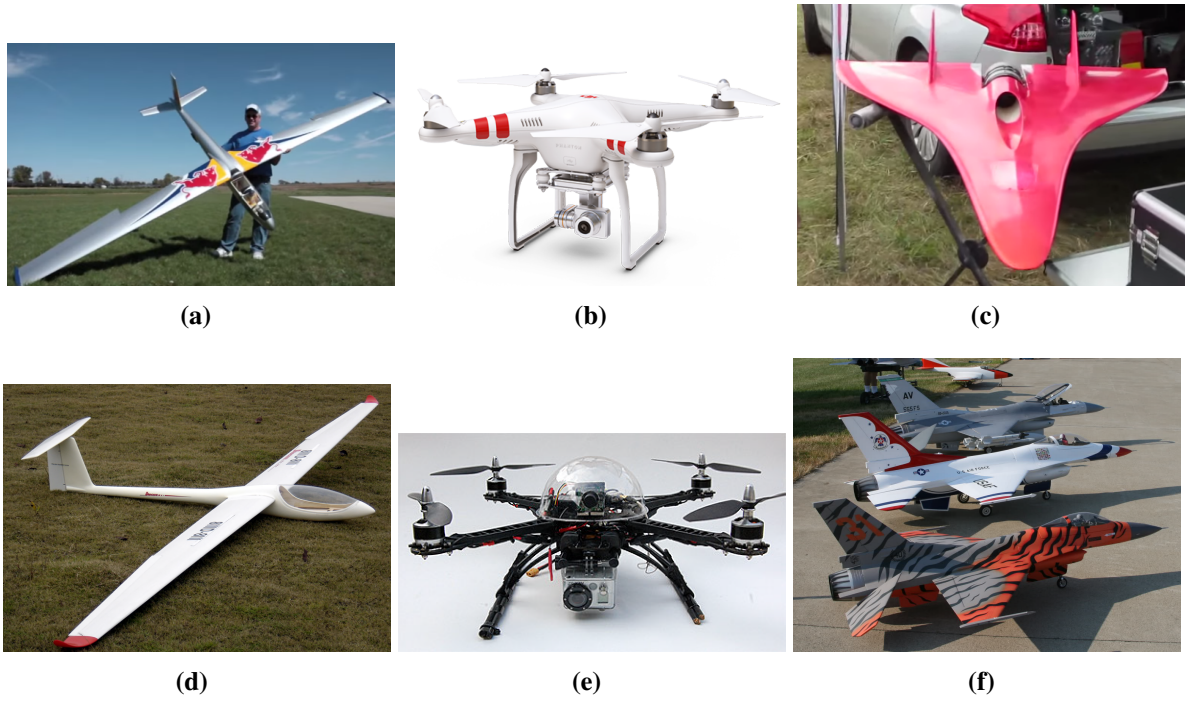
Class	Category	Operating Altitude (AGL)	Mission Radius	Payload
Class I (<150 kg)	Micro (<2 kg)	To 90 m (300 ft)	5 km	0.2-0.5 kg
Class I (<150 kg)	Mini (2-20 kg)	To 900 m (3000 ft)	25 km	0.5-10 kg
Class I (<150 kg)	Small (<150 kg)	To 1500 m (5000 ft)	50-100 km	5-50 kg
Class II (150-600 kg)	Tactical	To 3000 m (10000 ft)	200 km	25-200 kg

Table 1. Definitions of drone types discussed in this report. These values are taken from the NATO LSS UAS detection report.

Our analysis focuses on technologies currently available in the market that are designed to detect Class I drones, with an emphasis on the micro and mini categories. This restriction in the overall threat scope limits the potential target capabilities to less than a mile in achievable altitude, a mission radius less than 50 km (62 mi), and a carrying payload less than 50 kg. Again, these capabilities are reduced further for the more prevalent mini and micro categories within Class I. The NIAG report also classifies slow targets as those capable of moving less than 10 m/s (22 mph), however, hobbyist drones using micro jet turbine engines can reportedly operate up to 111 m/s (250 mph).

2.2 Examples

Commercial UASs continue to grow in capability, with a variety of systems available for purchase from consumer RC aircraft sites. We offer two types of LSS UASs for consideration: a glider and a quadcopter. Additionally, a low, *fast*, and small UAS type that utilizes a miniature jet turbine is included as a more forward-thinking threat possibility. Two examples of each type are shown in figure 1.



(a) **(b)** **(c)**

(d) **(e)** **(f)**

Figure 1. Examples of commercially available LSS UAS. (a) and (d) show two variants of a glider type UAS, (b) and (e) show commercially popular quadcopters, (c) and (f) show jet turbine based high velocity UAS.

2.3 Threat Engagement

The UAS examples presented are considered threats if they have the potential to perform dangerous, malicious, or unwanted acts. This includes devices intending to carryout a hostile mission, being operated by an unsafe individual, or crossing into a sensitive area. UAS threats must be appropriately dealt with by security systems, where the type and extent of mitigation techniques depend on the situation and environment. Therefore, we broadly define three steps to UAS threat engagement:

1. **Detection** – The collection of some phenomenological information captured by a sensor. This step does not necessarily denote classification (that is, differentiation of nuisance alarm versus target).

2. **Classification** – Analysis of data received in the detection phase, with the goal being to separate real targets from highly cluttered, noisy background data. When this step is performed solely by a human, considerable care must be taken to understand how nuisance alarms affect classification performance.

3. **Neutralization** – Once a target is positively identified in the previous step, additional action must be taken to deny mission success, including the potential for target neutralization.

3 Detection Technologies

Several phenomenologies can be used to detect and identify a LSS UAS. These include:

- Reflectance of UV/Visible/NIR/SWIR/MWIR/LWIR photons
- Reflectance of a particular photon polarization state
- Radar reflectance
- Acoustic emission
- Electromagnetic emission from onboard radios, WiFi, altimeters, radar, or other communication links
- Induced magnetic field

We broadly define several categories of technologies that utilize these UAS phenomenologies for detection. The following list discusses the positive and negative attributes for these methods:

- Passive visible imaging (UV, visible, NIR)
  - Pros: Singular units inexpensive, numerous commercial options, flexibility with FOVs
  - Cons: Low target contrast possible, susceptible to clutter, requires an additional modality for large volume search, requires active illumination at night, susceptible to weather degradations
- Passive thermal imaging (SWIR, MWIR, LWIR)
  - Pros: Reduces background clutter (only see things with thermal signature), works well at night, less susceptible to weather degradations
  - Cons: Most UAS have low thermal signature (See NIAG report), requires an additional modality for large volume search
- Active Time of Flight systems (LIDAR, range gate imaging, etc)
  - Pros: Very accurate distance measurements over large range (kilometers), depending on design may operate without significant degradation in inclement weather, active systems generally increase the signal-to-noise ratio, capability to operate both day and night
  - Cons: Expensive, scanning a hemisphere may take significant amount of time, accurate depth maps still require separation of target and background clutter, likely not eye safe
- Acoustic based sensors
  - Pros: Inexpensive, passive

  - Cons: Unknown max detection range, identification of drone may require storing a library of known signatures, nuisance alarm rate unknown in the urban environment, wind will change max range

- RF emission
  - Pros: Relatively inexpensive, most commercial drones emit easily detectable signals
  - Cons: Cannot address a quiet threat

- Radar based systems
  - Pros: Versatile technologies to detect and track targets of a variety of size over kilometers of distance, hemisphere scanning at modest refresh rates possible, many systems high TRL
  - Cons: Unknown drone radar cross section, identification can be difficult with just radar

- Magnetic detection systems
  - Pros: Can detect UAS if substantially large metal parts are used
  - Cons: Most LSS UAS use minimal metal parts, unknown maximum detection range, unknown noise characteristics in the urban environment

- Human intelligence
  - Pros: Unparalleled classification performance, able to initiate neutralization techniques
  - Cons: Demonstrably poor performance for long term monitoring in high consequence, low probability of event situations, costly

The UAS examples from the previous section have unique characteristics or abilities that challenge the engagement process, specifically detection and/or identification. These challenging qualities are generally affiliated with one or more of the low, slow, and small attributes. For the three UAS types under consideration, the challenges are noted as follows:

- **Glider UAS made with radar transparent materials** – Very small radar cross section, very low thermal signature, potentially camouflaged to visible cameras, low/no acoustic signature, very few metal components.

- **Quadcopter UAS** – Small radar cross section, commercially prevalent, requires limited and easily acquired knowledge to pilot, mild acoustic signature, newest quadcopter UASs can be automated with limited to no human control.

- **Jet turbine based UAS** – Small radar cross section, can reach extremely high speeds (compressed response timeline), components readily available for purchase online.

The ability to detect these UASs with conventional technologies is summarized in table 2, where green, yellow, and red indicators represent good, mild, and poor detection performance, respectively. The lack of green indicators for all UAS types is supported by the findings of the NATO study, namely that multiple detection technologies must be integrated or fused into a single detection/classification architecture to ensure higher probability of detection.

Detection scheme	Glider	Quadcopter	Jet
Radar			
Passive optics (i.e., cameras)			
Active optics (i.e., LIDAR)			
Acoustics			
EM emissions			
B-field detection			

Table 2. Ability to detect typical UAS types based on conventional sensors.

4 Effectors and Mitigation Strategies

Once a LSS UAS is detected and identified as a threat, target mitigation begins. We broadly define mitigation as denial of mission, including the potential destruction of the LSS UAS target. The NATO SG-170 report makes several important statements regarding effector choice:

- "Some types of weapon systems may not be appropriate because of safety constraints and the risk of collateral damage near to civilian infrastructure during peace-time."
- "The interception range, or the range of influence of an effector, must be greater than the potential stand-off range of the UAV, in the event that the UAV is carrying a threat payload (i.e. the UAV is not the payload itself)."
- The effector may dictate requirements of the sensor. For instance, certain detectors may require target designation, tracking, and high sampling rate. This is also true in the opposite direction, where the most effective sensors may restrict the type of mitigation methods. In essence, the two must complement one another so that the system is most effective.

We broadly classify five types of effectors that could be used to deny an LSS UAS mission: missiles, guns, laser systems, electronic counter measures/high power microwave/high power electromagnetic weapons, and non-destructive techniques.

Ultimately, the appropriateness of the methods for mitigation or neutralization of LSS UAS targets within the desired setting is what will dictate their use and/or implementation in future GBAD systems or LSS UAS mitigation systems. For instance, the use of airburst ammunitions and missiles for security or safety protection is obviously not ideal in a heavily populated civilian environment. On the other hand, these methods may be appropriate for engaging targets on a hostile battlefield. The decision for use of such devices must be heavily influenced by the inherent risks in each (e.g. collateral damage or ineffectiveness), and whether the consequences of those risks are determined to be acceptable.

4.1 Missile effectors

Guided missile systems can be classified based on the guidance principles. The first is Command Line of Sight (CLOS) systems, which require that the system track both the target and the missile. The guidance commands are transmitted (via radio command link or beam) to the missile. Therefore, line of sight is required throughout the engagement. In the context of UAV defense, the performance is dependent on the ability of the ground based tracking elements to accurately track the LSS threats.

Several type of seeker guidance systems are employed within the missile system. The IR seeker locks the missile onto warm elements of the target. Small, low emission targets against complex backgrounds are more difficult, however. The trend is to transition towards imaging sensors to

improve performance, but the costs will increase. Similarly, the RF seeker locks-on to RF radiation. For LSS targets, there is a concern that this missile's reliance on Doppler filtering to extract low targets from ground clutter could limit its effectiveness. Finally, semi-active laser (SAL) seeker technology could be applicable but has not yet been applied to GBAD systems.

NATO SG-170 generally accepts that a single missile can destroy an LSS target given adequate lock-on and stable tracking. However, no (unclassified) data is listed in the report to support the guidance and tracking requirements. The document further states, "There is confidence in current and future systems having adequate guidance capability. However, there are acknowledged detection and fusing challenges against micro UAVs." Furthermore, the potential risk for drastic collateral damage in urban or sensitive environments draws very serious doubts about the appropriateness of this effector type for many applications outside of military combat.

4.2 Guns and Ammunition

NATO lists three categories: machine guns (5.56-12.7 mm), cannon guns (20-57 mm) and low fire guns (76 mm). All of these are dependent on sensors for tracking and target identification. Machine guns are deemed unsuitable for the LSS threat due to poor accuracy and range performance, though performance can be improved with additional techniques.

Cannons are already used in GBAD systems but are only effective against LSS targets using airburst ammunition. Micro UAVs are still an exception that may require significant amounts of ammunition for a high kill probability. Low fire rate guns seem ineffective against LSS targets, particularly swarm attacks.

Guns can be effective against LSS targets, particularly with airburst ammunition that assumes a well-established target track, but may have limitations for micro UAVs. The number of rounds required is proportional to the costs, but this is expected to be below the costs of a standard missile. In addition, the type of ammunition and the suspected amounts required for a kill are undesirable for urban and high-consequence environments.

4.3 Laser systems

Several laser options exist that require a direct line of sight for effectiveness. Varying degrees of effectiveness are achievable, but generally have increased cost for increasing confidence in effectiveness.

Low-power lasers are intended to "dazzle" or destroy electro-optical sensors mounted to the target. For effectiveness, the laser must be in the field of view and in the transmission band of the sensor (i.e. a stop-band filter could potentially block transmission). Assuming transmission through the optics, increased power can disrupt or damage the optical sensor. UAS that rely upon optical sensors for flight control could potentially be defeated by low-power lasers.

Pulsed, medium-power lasers have enough energy per pulse to damage or destroy the first optical surface of the platform, rendering the optical system inoperable.

High-energy lasers are generally capable of defeating the target structure, but this also depends on the target construction, material, and range. Several technologies are currently under investigation, with fiber lasers getting much attention due to their flexibility and compactness.

NATO SG-170 notes that several programs have demonstrated the ability to destroy in-flight UAVs with 10's of kilowatts at ranges greater than 2 kilometers. Environmental conditions (e.g. rain, snow, fog, etc.) can dictate performance, though the target must also be capable of withstanding the same environmental conditions. These limitations may also be less severe in the likely short-range scenarios for LSS threats. Lasers have a large upfront cost driven by the maximum operating range and the necessary power, but subsequent use costs per engagement are much less. Collateral damage is minimized by precisely focusing the beam on the target.

4.4 Electronic Counter Measures, High Power Microwave, High Power Electromagnetic Weapons

Electronic counter measures (ECM), high power microwave (HPM), and high power electromagnetic weapons (HPEW) are designed to transmit electromagnetic signals somewhere in the frequency range from 10 kHz up to several GHz. Power levels range from several watts up to gigawatts, depending on the technology. ECM applied to the LSS target set is mostly dedicated to interfering with any RF receiver. Susceptible systems are identified as the avionics systems (e.g. altimeters), data and command links, SAR and D/GMTI radar, commercial mobile telephony, personal mobile radios (AM/FM), and global positioning systems (GPS).

The goal of radar ECM is to prevent successful reception or transmission of data. This may mean simple narrowband jamming (denying the platform the use of the jamming spectrum) or more sophisticated approaches.

Comms ECM aims to exploit information contained within the data-link, which is more similar to a cyber style attack. Details about this technique could not be included in the NATO report due to the security classification. However, the time durations of such attacks must be considered, especially in the case of a swarm attack, where isolating individual targets may be too difficult for an intelligent attack strategy.

Altimeters are more likely to be used by nation states, and may be difficult to penetrate. Personal communication devices are very vulnerable to simple jamming techniques but this will likely interfere with any nearby civilian or friendly systems.

GPS ECM, consisting of jamming or spoofing, is simple due to the weakness of GPS signals. However, protection techniques are available to amplify the satellite signal and attenuate in the direction of the jamming signal. Spoofing is noted as more effective but also more difficult.

HPM and HPEM can be very effective, with effects ranging from temporary disruption to

physical destruction of unprotected electronics. External factors, such as the electric field strength in the target area, the frequency, and the target shielding capabilities, also influence this method's effectiveness. This mitigation strategy has low directivity and thus has an advantage in that it does not need precise target location or tracking. However, the low directivity also means that coalition systems would also likely be affected if left unprotected. This strategy can engage many LSS threats before recharging, however, it has never been included in a GBAD system, and no public data is available for the operational range.

Though ECM technologies are likely to be effective against low-cost, consumer grade LSS threats, there is a certain degree of risk that the sophistication level of the on-board electronics could prevent effective mitigation. Undesirable collateral damage to civilian or friendly electronics is also possible. GPS and remote control communications link jamming/spoofing are existing technologies that can be effective for LSS targets that rely upon one or both for navigation.

4.5 Non-destructive techniques

A host of non-destructive denial techniques exist that may be appropriate for some LSS UAS threats. While these may be sub-optimal solutions for a battlefield situation, they may be better suited for the urban environment.

Various nets fired at LSS UAS targets could be utilized to deny mission. Typically seen are human operated net cannons designed to capture a group of birds. While other net based systems have been discussed, the use cases, particularly the time to respond and deny, have not been thoroughly discussed. Maximum net firing range is limited, likely in the tens of meters. Some companies have utilized a UAS controlled by an operator that deploys a net onto the target. These systems are limited by the user and the physical capabilities of the intercepting UAS with the net system installed on it. The system is contingent on the intruding UAS being relatively stationary and slower than the intercepting UAS. If the intruding UAS is being flown by a more skilled pilot, or is faster than the intercepting UAS, the net scheme will be circumvented.

Water cannons are a potential non-lethal technique that could be used to deny an LSS UAS system. Systems currently exist targeted towards firefighting and anti-piracy applications for commercial shipping vessels. While these systems may be used to defeat LSS UAS, there is no comprehensive system that integrates a water cannon to effectively track and lock-on to a target. Maximum range for these systems are likely limited to the 50-100 meter range.

Other less explored options may include the use of SNL developed sticky foam, or trained raptors to attack LSS UAS targets.

5 Key NATO study findings

The NATO Industrial Advisory Group Study SG-170, "The Engagement of Low, Slow and Small Aerial targets by GBAD" is the fifth study in a series spanning ten years. The SG-170 study, published in October, 2012, and updated nine times, most recently in July, 2013, is a comprehensive study of detection, classification, and effectors available to address the LSS UAS threat. Due to the size of the document, a summary of key findings is presented.

The NATO study found compelling evidence on the complications of UAS detection due to the physical size of UAS and minimal detection phenomenology. It was stated in the report, "The challenge for LSS threat detection for current high frequency sensors is the false alarm plots and how to engage with the real LSS threats that are in the velocity domain of clutter or natural objects such as birds, 'angels' or ground vehicles. The combinations of sea and land clutter, climatic and atmospheric anomalies are compounded by the high number of real contacts varying from large qualities of birds to surface and air objects in a congested battle space."

Compounding the difficulty of detecting a UAS within a cluttered environment, UAS are generally difficult to detect. The radar cross section (RCS) for two small commercially available platforms was measured to be -15dBm^2 and is theorized to be -30dBm^2 if the UAS is constructed with an RF transparent material. Imaging commercially available quadcopters with EO/IR visible, MWIR, and LWIR resulted in low contrast images, and the amount of data required to provide a reasonable response time is very large. Acoustic detectors were successfully demonstrated and identified a UAS from 25 meters at an elevation of 10 meters using a microphone array (ambient wind was cited as the major reason for such reduced detection range with acoustics in this field test). RF detection is promising since currently available COTS UAS technology requires a transmission and receive signal from a human user. The detection of RF becomes highly complicated if a UAS uses open source software or is programmed to require no human interaction. Disturbances within the magnetic field around a UAS has potential to be detected, but is dependent on the materials used and the physical size of the system.

The NATO report concludes by stating that urgent action is necessary if the operational risks from these platforms are to be minimized and states that the application of some innovative tactics and technologies to effectively counter these threats will be necessary. The mixture of traditional sensors used in GBAD systems and new technologies is stated as critical to build a robust system capable of solving the LSS UAS problem.

6 Survey Results- Detection and Identification Products

Each company identified as selling a product potentially relevant to the UAS detection, classification, and neutralization problem is listed below. Major products are identified, and underlying methods of operation are shown in blue text. For additional information, including pictures of subsystems, see appendix A.

Liteye

- System name: Anti UAV Defense System (AUDS)
  - Blighter Surveillance Systems (UK)
    - Blighter A400 series air security radar
      - 90° or 180° HFOV; 10° or 20° VFOV (±40° with added hardware)
      - E-scan frequency modulated continuous wave Doppler radar; Ku frequency band ("ideally suited to detecting the small structures used to construct compact UAVs" (cite http://www.blighter.com/products/a400-series-radars.html)
      - Max ranges: micro- 2 km (1.2 mi), mini- 3 km (1.9 mi), large- 8 km (5 mi)
      - Min scan time: $\approx 90°$ per second
      - Min target size: RCS $= 0.01$ m^2(0.1 ft^2)
      - FAR: 1 per day (No details given)
    - "able to detect small UAVs in all weather conditions 24 hours a day"
  - Chess Dynamics (UK)
    - IR camera – Gen3 Cooled 0.33 MP, 3-5 μm (MWIR)
    - EO camera – color HD 2.3 MP, optical zoom x30, digital zoom x12, auto focus
    - Video tracking technology
    - "able to track the UAV and, combined with radar target information, classify the target"
    - Human makes decision to neutralize
  - Enterprise Control Systems (UK)
    - Smart RF inhibitor interferes with C2 channels
    - GPS L1, 915 MHz ISM, and 2.4 Ghz ISM (software defines frequency bands)
    - Range: 1-2 km (0.6-1.2 mi)
- Sources:
  1. Bligher AUDS Fact Sheet
  2. blighter.com
  3. enterprisecontrol.co.uk
  4. Notes from briefing by Liteye Systems, Inc. (Jan. 2015)

SRC

- Not-for-profit company formerly affiliated with Syracuse University
- System 1 name: Tactical Counter-UAS Technology (TCUT) System
  - AN/TPQ-50 radar w/ LSTAR air surveillance software
    - L-band, max range of 10 km (12 mi.), 0-30° elevation, 360° azimuth
    - Simultaneous tracking of multiple targets in 3D
    - Designed for detection and warning of RAM launchers
    - LSTAR software enables detection of "low altitude, slow flying, small radar cross-section targets like ultralights and paragliders/hang-gliders"
  - AN/ULQ-35 CREW Duke system
    - Uses EW jamming to neutralize remote controlled IED devices
    - Supports programming upgrades to adapt to evolving threat environment
  - EO/IR camera
  - Rule-based decision engine
  - Detects, tracks, provides visual and electronic identification, and delivers electronic negation capabilities
- System 2 name: SCEPTRE cUAS System
  - Partnered with US Army to develop capabilities for a complete solution
  - Adds lethal miniature aerial munitions to the TCUT system, providing a kinetic negation capability
- Radar system name: SR Hawk (V)3 Multi-Mission Radar
  - Small and lightweight package size, low cost, low power
  - 360° scanning
  - Can integrate camera and GPS
  - All weather - "suppressing clutter from rain, snow, sea and tower sway"
  - "Low false alarm rate"
- "We have successfully demonstrated our capabilities to detect, track, identify and negate UAS at [Black Dart]."
- Sources:
  1. srcinc.com
  2. AN/TPQ-50 Counterfire Radar Product Overview Sheet
  3. AN/ULQ-35 CREW Duke Product Overview Sheet
  4. SR Hawk (V)3 Multi-Mission Radar Product Overview Sheet

DeTect

- Known for advanced bird radar technologies and wind measurement radar but also have security and surveillance products
- Small company based in Panama City, FL
- CTO Adam Kelly recently featured in IEEE Spectrum article due to recent events
  - (Paraphrasing) "Trick is not in sensing the subtle radar return but distinguishing a small drone from the many birds that will also be sensed"[1]
- System name: HARRIER Drone Surveillance radar DSR-200
  - S or X-band Doppler radar
  - Based on avian radar technology; optimized for small targets
  - Employs machine learning for classification based on about 50 data tags (e.g. size, speed, heading, time, date, alone/swarm, etc.)
    - Kelly claims most advanced radar processing being done for radars
    - Takes time to "learn" migration patterns
    - Automatic false positive (birds) rejection
  - "most sensitive and advanced system available for detection, tracking, and interdiction of drones and small UAVs" - company website
  - Provides visual and audible notification
  - Compatible with other security and display systems
  - Customizable with video and thermal options
- Sources:

1. D. Schneider. *Can We Detect Small Drones Like the One That Crashed at White House? Yes, We Can.* IEEE Spectrum. Feb 2015.
2. HARRIER Security Radars Technical Data Sheet
3. HARRIER DSR-200 Technical Data Sheet

Torrey Pines Logic

- Active scanning optical system looking for targets performing surveillance
- System name: Beam 200
  - Active optical system that looks for retro-reflections from optics
    - Detection of cameras and scopes

    - Minimum detectable size is unclear, but would not detect cell phone camera sized systems
  - Spectral band unknown
    - "Multi-spectral imaging for target verification"
    - Likely NIR laser illumination
  - Max range: 1 km
  - Elevation: -30° to +90°; Azimuth: continuous 360° scan
  - Scan time unknown; states "at video rates" (Beam 100 system scans at 60°/sec)

- Sources:

  1. tplogic.com
  2. Beam 200 Brochure

IEC Infrared Systems

- System name: Narcissus Optical Augmentation System
  - Active scanning optical system looking for retro-reflections from multi-layered optics like scopes, binoculars, or cameras
  - Detection triggers long range EO/IR assessment camera for classification and geo-location of target
  - Max range and field of views unknown
  - Minimum detection size unknown

- System name: Banshee
  - Uncooled LWIR 360° thermal image in "all weather conditions" (human detection at 300 m)
  - IEC Werewolf assessment camera identifies threat
  - Counter tactics include 12 million-candle spotlight, laser pointer, and LRAD

- Other integrated options include additional neutralization methods (Dragon Escalation of Force, Hornet)

- Sources: iecinfrared.com (Narcissus) and iecinfrared.com (Banshee)

Dedrone

- Relatively new, German company
- System name: DroneTracker
  - Passive visible imaging, acoustics, ultrasonics, and video motion detection (VMD)
  - "Reliable" detection within 100 m (330 ft)
  - Classification at 70m (230 ft)
  - Day and night detection; completely independent of noise emission
  - Several DroneTrackers can interact and provide an extended range
  - Automated comparison with a central database
  - Wireless connection
  - No mitigation
- Source: dedrone.com

DroneShield

- Microphone measurements with signal processing determine the presence of a UAV based on parasitic acoustic signature
  - Omnidirectional: 300° FOV, short range
  - Parabolic dish: 30° FOV, increased range
  - Max range depends on many factors (UAV type, noise environment, dish vs. omnidirectional, etc.)
  - Example: DJI Phantom, suburban environment
    - Omnidirectional: approximately 150 m (500 ft)
    - Parabolic dish: approximately 1 km (0.6 mi)
- Identification and classification are based on acoustic spectral content and how well that matches a database entry
  - Database is updated quarterly
  - Some form of pattern matching
  - Company's website suggests one signature will not detect other new devices if fundamental frequency is different
- Asked to participate in Black Dart 2014
- Source: droneshield.org

Orelia

- Small French company founded in 2007
- Claim to be experts in audio pattern recognition, machine learning, and signal processing
- System name: Drone Detector
  - Microphone detection of generic acoustic signature generated by electric propeller UAVs (fixed or rotary wing)
  - Recommended installation on flat, sound-reflective surface 3 m (10 ft) high
  - Longer range when background noise floor is less than 40 dB
  - Ethernet cable connection for communication and power
  - Alarm also available from contact inside the module
- Source: drone-detector.com

CellAntenna

- Solutions to enhance or prohibit cell phone signals
- Based in Coral Springs, FL with offices in Europe
- System name: Drone Detection and Defeat Technology (D3T)
  - RF emission of controller and video signals
  - Max range: 1-2 km (0.6-1.2 mi) standoff distance, 300 m (1000 ft)
  - Antennas deployed within and at the fence line form a "bubble" of protection, not affecting systems outside
    - "Does not interfere with RF communication"
    - Scalable to cover large areas
  - Signal is processed to determine the type of flight control system
  - Electronic countermeasure capabilities:
    - Taking control of the target (full control, land suddenly, send back to origin, etc.)
    - Depriving accurate GPS data
    - Simultaneous deployment of multiple countermeasures
    - Other proprietary techniques
- Source: H. Melamed (CellAntenna CEO), M. Ponce, M. Horvat, and C. Svanberg. *Understanding the Terrorist Threat of Hobbyist Drones – Government Agency Edition.* April 2015.

Domestic Drone Countermeasures (DDC)

- Very small company founded in 2013, in Oregon City, OR (website has a Kickstarter link)
- System name: Basic Drone Detection System
  - RF emission device network that triangulates unknown receivers within a mesh grid of sensors
  - Detection of RF transmitters in the range of 1 MHz – 6.8 GHz
  - Ignores manual list of known transmissions
  - Expandable coverage by adding sensor notes
  - Each node can detect within 50 ft in all directions
- Source: ddcountermeasures.com

7 Survey Results- Mitigation and Denial Products

Mitigation and denial of mission products include both destructive and non-destructive systems. Several of these systems straddle the COTS/GOTS domains

Rheinmetall

- German automotive parts supplier and military technology group
- System name: Skyshield air defense system
  - High energy laser that uses beam superimposing technology
  - Max range: 3 km (1.9 mi)
  - Rheinmetall Live Laser Demonstration 2013
    - "Successful engagement of a swarm of jet-powered droned by a stationary Skyshield air defence system, whose effectiveness likewise relies on a HEL effector" (targets flew into the target zone one after the other)
    - "Demonstrated a complete kill-chain capability against vertical take-off UAVs"
    - A radar detects and identifies the targets, then the rough and fine tracking is performed by the HEL system
    - Range of demonstration not given
- Source: rheinmetall-defence.com

Raytheon

- System name: Vigilant Eagle
  - Illuminates the missile body with electromagnetic energy tailored to divert the missile
  - In 2007, had already been working on for over 10 years
  - In 2006, awarded $4.1M from DHS to demonstrate the suitability to function in a civilian environment
  - 3 primary components:
    - Distributed missile detect and track sub-system (MDT) – pre-positioned grid of passive infrared sensors mounted on cell phone towers or buildings to cover the required detection space
    - Command and control (C2) system – providing pointing commands and connects to airport security; determines missile launch point;
    - Active Electronically Scanned Array (AESA) – Created electromagnetic fields are well within the Occupational Safety and Health Administration (OSHA) standards for personnel exposure limits.
- Source: raytheon.com

Thales Group

- System name: Green Laser Optical Warner (GLOW)
  - Gun-mounted, intense green light to warn
  - Narrow (long range) or wide (close range) beam choice; narrow beam diameter is 0.5 m at 50 m range; wide beam will "fill a car window"
  - No proof of use against optics
- Sources: wired.co.uk and thalesgroup.com

BAE Systems

- System name: CIRCM
  - Integrated aircraft protection solution for infrared-guided threats
  - "employs next-generation laser-jamming capabilities"
  - Lighter, more advanced version of the ATIRCM system
    - ATIRCM detects a missile, reject false alarms, cues infrared jamming system to the missile location, and emits high-energy infrared beam to defeat the missile's IR seeker
- Sources: baesystems.com (CIRCM) and baesystems.com (ATIRCM)

MALOU Tech

- French company selling UAS with attached net
- Uses pilot to intercept UAS
- Source: MALOU-Tech link

Delft Dynamics

- Netherlands based small business
- Demonstrated a UAS-based net cannon system
- Source: DelftDynamics.com

8 Conclusion

LSS UAS detection, identification, and mitigation is a challenging problem. Systems exist in the commercial domain that likely solve a limited piece of the larger LSS UAS problem, but no complete system appears to exists with evidence of acceptable performance.

Based on the results of our market survey, we recommend the testing and evaluation of products from the following companies:

- Liteye
- SRC
- DeTect
- DroneShield
- CellAntenna

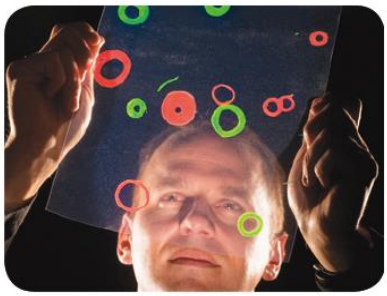
These companies are recommended for investigation based on their turn-key system approach (Liteye, SRC), novel machine learning strategy to separate LSS UAS from background clutter (DeTect), use of acoustic detection (DroneShield), and detection and mitigation through electronic countermeasure techniques (CellAntenna).

Ultimately, the detection of a range of LSS UAS types will require multiple modality, data fusion systems to effectively detect and identify targets amongst a cluttered background.

A PowerPoint presentation

Exceptional service in the national interest

Sandia National Laboratories


UAS Detection/Mitigation Market Survey

Gabriel Birch, John Griffin, Matthew Erdman
Sandia National Laboratories
April 20, 2015

U.S. DEPARTMENT OF ENERGY | NNSA National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND2011-0439P

Sandia Proprietary

Overview

Sandia National Laboratories

- Summary: UAS detection and neutralization is a hard problem
  - Hard to detect and classify threat
  - Plausible threat definition can vary drastically in transportation modalities and in their payload capabilities
  - Hard to neutralize threat once detected and classified
- UAS examples
  - Low Slow and Small (LSS)
- Detectable phenomenologies
  - Radar, active and non-active optics, acoustics, RF emission, and possibly magnetic response
  - All modalities have strengths and weaknesses
- NATO report summary
- The confusion with vendors
- Market survey results to date

UAS examples

Sandia National Laboratories

Class	Category	Operating Altitude (AGL)	Mission Radius	Payload
Class I (<150 kg)	Micro (<2 kg)	To 90 m (300 ft)	5 km	0.2-0.5 kg
Class I (<150 kg)	Mini (2-20 kg)	To 900 m (3000 ft)	25 km	0.5-10 kg
Class I (<150 kg)	Small (<150 kg)	To 1500 m (5000 ft)	50-100 km	5-50 kg
Class II (150-600 kg)	Tactical	To 3000 m (10000 ft)	200 km	25-200 kg

- Low, slow, small (LSS) UAS

Commercially available quad copter. Inexpensive, autonomous.
(DJI Phantom 2, ~$1k)

Gliders built from radar transmissive materials.
~2k$

Mini-jet turbine engines, ~$3k, max speed of 250mph (World record at 440mph)

Detection phenomenologies

Sandia National Laboratories

			
Passive (i.e., cameras)			
Active (i.e., LIDAR)			
Reflectance of radar			
Acoustics			
EM emissions (WiFi, altimeters, communication links, etc)			
B-field detection (magnetics)			

NATO Report Summary

Sandia National Laboratories

- (NATO) Industrial Advisory Group Study SG-170, "The Engagement of Low, Slow and Small Aerial targets by GBAD"
  - 5th study, spanning 8 years, published in 2013
- LSS UAS detection techniques and mitigation techniques
- Discussion of civilian attack concerns
  - "Even short-range mini-UAVs with simplistic effectors such as light automatic guns have the potential to create havoc and major psychological and media impact."
- "No sensor type provides a sufficient tracking and identification capability used by itself against the LSS threat."
  - Goes on to state the need for sensor data fusion

NATO Report Summary (con't)

Sandia National Laboratories

- "In light of the gaps at the effector and sensor level, it is proposed that a further study should be conducted to examine the optimum sensor/effector mix to counter the LSS evolving threat."
- "To provide a satisfactory performance, the use of an adequate mix of sensors will be crucial."

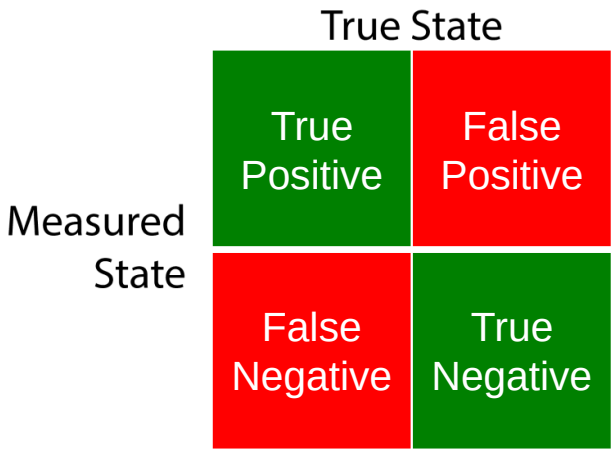
Conclusion: "Urgent action is necessary if the operational risks from these platforms are to be minimized and it requires the application of some innovative tactics and technologies to effectively counter these threats."

Confusion (matrix)

- "We detected everything they threw at it."

Equals high true positive rate, only a part of the bigger picture.

What is the false positive rate? Testing in a realistic cluttered environment?



- Detecting targets is not the hard part. Differentiating them from the background clutter is the problem.
  - Low, slow, small doesn't help the detection problem
- No hard evidence for most vendor claims
  - If you don't have a confusion matrix, you don't have any knowledge if it will work.

Market Survey- Detection/Classification

Sandia National Laboratories

- Three predominant sensor modalities on the market
  1. Radar
  2. Imaging (active and passive)
  3. Acoustics
  - Some notable systems using RF emission.
- Radar is the strongest and most widely marketed modality and appears to have a limited number of well known companies in the market
- Other technologies such as acoustics and RF emission detection have promising, but limited results
- Most radar system using an optical system as a means to classify threat
  - Consider the swarm

Market Survey- Detection/Classification

Sandia National Laboratories

System Name	Modality	Range	Notes
Falcon Shield	Radar/Optical (?)	Unknown	Used at 2012 Summer Olympics
Liteye	Radar/Optical/ Jamming	Up to 6km	
SRC	Radar/Optical/ Jamming	Up to 50km	Used at 2012 Summer Olympics, G8 Summit, and US Marine Corp.
DeTect	Radar	3km for styrofoam UAS	Machine learning capability

Market Survey- Detection/Classification

Sandia National Laboratories

System Name	Modality	Range	Notes
Torrey Pines Logic	Active Imaging	1km	Scans a laser looking for reflections from optics.
IEC Infrared Systems	Active Imaging	Unknown	Similar to Torrey Pines Logic.
Dedrone	Passive Imaging + Acoustics + Video Analytics	100m	Goal of 500m detection. Uses a company created library of UAS shapes/sounds.

Market Survey- Detection/Classification

System Name	Modality	Range	Notes
DroneShield LLC	Acoustics	150m	
Orelia	Acoustics	Up to 100m	
CellAntenna	RF Emission	Up to 6km	Jamming capabilities
DDC LLC	RF Emission	100ft diameter per sensor	

Mitigation Techniques

Sandia National Laboratories

- NATO general statements
  - Some weapon systems are inappropriate because of safety constraints and the risk for collateral damage
  - An effective mitigation scheme may dictate the sensor type
    - Requirements for target designation, tracking, and sampling rates
    - Also true that most effective sensors may restrict mitigation methods
    - Sensing and mitigating techniques should complement one another
- Mitigation types (effectors):
  - Missiles
  - Guns and ammunition
  - Laser weapons
  - Electronic counter measures
- Appropriateness of methods for mitigation of LSS threats within the desired setting will dictate use
  - Example: airburst ammunition not ideal for civilian environment but more appropriate for hostile battlefield
  - Decision for use heavily influenced by the inherent risks in each and corresponding consequences of those risks

Summary

Sandia National Laboratories

- LSS (or LFS) UAS detection is very difficult
  - To this point, not a lot of investment for this particular problem
- Mitigation requires collateral damage trade off
- Liteye, SRC, DeTect, DroneShield, CellAntenna
- Not just an incremental improvement of technology to detect/mitigate
  - This is a differentiation problem, and will require data fusion, potentially even machine learning

Multiple commercial entities worth investigating, but need unbiased, quantitative tests in realistic environments

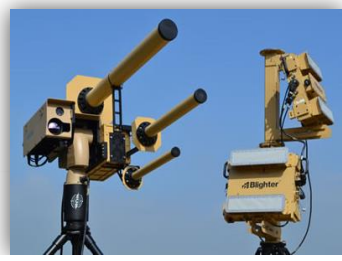
More Survey Information

Sandia National Laboratories

See slides that follow

Liteye

- Anti UAV Defense System (AUDS)
  - Blighter Surveillance Systems (UK)
    - Blighter A400 series air security **radar**
      - 90˚ or 180˚ HFOV; 10˚ or 20˚ VFOV (+/- 40˚ w/ added hardware)
      - E-scan frequency modulated continuous wave Doppler radar; Ku frequency band ("ideally suited to detecting the small structures used to construct compact UAVs"[1])
      - Max ranges[2]: micro- 2 km (1.2 mi), mini- 3 km (1.9 mi), large- 8 km (5 mi)
      - Min scan time: ≈90˚ per second
      - Min target size: RCS = 0.01 m^2 (0.1 ft^2)
      - FAR: 1 per day – In what environment?
    - "able to detect small UAVs in all weather conditions 24 hours a day"[3]
  - Chess Dynamics (UK)
    - **IR camera** – Gen3 Cooled 0.33 MP, 3-5 µm (MWIR)
    - **EO camera** – color HD 2.3 MP, optical zoom x30, digital zoom x12, auto focusVideo tracking technology
    - "able to track the UAV and, combined with radar target information, classify the target"[3]
    - Human makes decision to neutralize
  - Enterprise Control Systems (UK)
    - Smart **RF inhibitor** (jammer) interferes with C2 channels
    - GPS L1, 915 MHz ISM, and 2.4 GHz ISM (software defines frequency bands)
    - Range : 1-2 km (0.6-1.2 mi) [4]



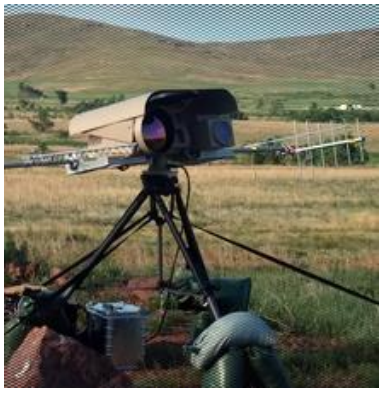
[1] http://www.blighter.com/products/a400-series-radars.html
[2] "highly dependent upon construction of the airframe and of the onboard electronics and payload"
[3] http://www.enterprisecontrol.co.uk/index.php?url=products_details&products_id=101&cat_id=34&id=34
[4] Briefing notes from Liteye Systems, Inc. (Jan 2015)

SRC

Sandia National Laboratories

- Not-for-profit company formerly affiliated with Syracuse University
- Tactical Counter-UAS Technology (TCUT) System
  - AN/TPQ-50 **radar** w/ LSTAR air surveillance software
    - L-band, max range of 10 km (12 mi), 0-30˚ elevation, 360˚ azimuth
    - Simultaneous tracking of multiple targets in 3D
    - Designed for detection and warning of RAM launchers
    - LSTAR software enables detection of "low altitude, slow flying, small radar cross-section targets like ultralights and paragliders/hang-gliders"
  - AN/ULQ-35 CREW Duke system
    - Uses **EW jamming** to neutralize remote controlled IED devices
    - Supports programming upgrades to adapt to evolving threat environment
  - **EO/IR camera**
  - Rule-based decision engine
  - Detects, tracks, provides visual and electronic identification, and delivers electronic negation capabilities

- SCEPTRE cUAS System
  - Partnered with US Army to develop capabilities for a complete solution
  - Adds lethal miniature aerial munitions systems to provide a kinetic negation capability to the TCUT system
- SR Hawk (V)3 Multi-Mission Radar
  - Small and lightweight package size, low cost, low power
  - 360˚ scanning
  - Can integrate camera and GPS
  - All weather - "suppressing clutter from rain, snow, sea and tower sway"
  - "Low false alarm rate"



- "We have successfully demonstrated our capabilities to detect, track, identify and negate UAS at [Black Dart]."

DeTect

- Company attributes:
  - Known for advanced bird radar technologies and wind measurement radar but also have security and surveillance products
  - Small company based in Panama City, FL
  - CTO Adam Kelly recently featured in IEEE Spectrum article due to recent events
    - (Paraphrasing) “Trick is not in sensing the subtle radar return but distinguishing a small drone from the many birds that will also be sensed”[1]

- HARRIER Drone Surveillance Radar DSR-200
  - S- or X-band Doppler radar
  - Based on avian radar technology; optimized for small targets
  - Employs machine learning for classification based on about 50 data tags (e.g. size, speed, heading, time, date, alone/swarm, etc.)
    - Kelly claims most advanced radar processing being done for radars
    - Takes time to “learn” migration patterns
    - Automatic false positive (birds) rejection
  - “most sensitive and advanced system available for detection, tracking, and interdiction of drones and small UAVs” – company website
  - Integration:
    - Provides visual and audible notification
    - Compatible with other security and display systems
    - Customizable with video and thermal options

[1] D. Schneider. *Can We Detect Small Drones Like the One That Crashed at White House? Yes, We Can.* IEEE Spectrum. 3 Feb 2015.

Torrey Pines Logic

Sandia National Laboratories

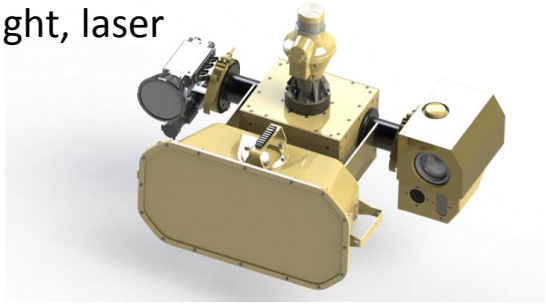
- Beam 200
  - **Active optical** system that looks for retro-reflections from optics
    - Detection of cameras and scopes
    - Minimum detectable size is unclear, but not good with cell phone cameras
  - Spectral band unknown
    - "Multi-spectral imaging for target verification"
    - Likely NIR laser illumination
  - Max range: 1 km
  - Elevation: -30˚ to +90˚; Azimuth: continuous 360˚ scan
  - Scan time unknown; states "at video rates"
    - Beam 100 system scans at 60˚/sec

IEC Infrared Systems

Sandia National Laboratories

- Narcissus Optical Augmentation System
  - Looks for multi-layered optics (scopes, binoculars, cameras)
  - Detection triggers long range **EO/IR** assessment camera for classification and geo-location of target
  - Max range and field of views unknown
  - Minimum detection size unknown

- Banshee
  - Uncooled LWIR 360˚ **thermal** image in "all weather conditions"
    - Human detection at 300 m (0.2 mi)
  - IEC Werewolf assessment **camera** identifies threat
  - Counter tactics include - 12 million-candle spotlight, laser pointer, and LRAD
- Other integrated options include additional neutralization methods
  - Dragon EOF (Escalation of Force)
  - Hornet



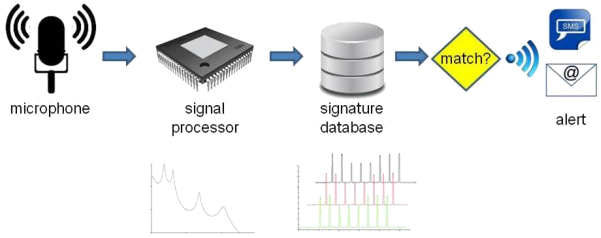
Dedrone

- German company
- DroneTracker
  - “Reliable” detection within 100 m (330 ft)
  - Classification within 70 m (230 ft)
  - Day and night detection; completely independent of noise emission
    - EO camera
    - Potential illumination for night
  - Sensor types and specifications unclear
    - Some mixture visible camera, acoustics, thermal, and VMD
  - Several DroneTrackers can interact and provide an extended range
  - Automated comparison with a central database
  - Wireless connection
  - No mitigation

DroneShield

Sandia National Laboratories

- Microphones and signal processing determine the presence of a UAV based on it's parasitic acoustic signature
  - Parabolic dish: 30˚ FOV, increased range
  - Omnidirectional: 300˚ FOV, short range
- Max range depends on many factors (UAV type, noise environment, dish vs. omnidirectional, etc.)
  - Example: DJI Phantom, suburban environment
    - Parabolic dish ≈ 1 km (0.6 mi)
    - Omnidirectional ≈ 150 m (500 ft)
- Identification and classification are based on acoustic spectral content and how well that matches a database entry
  - Database is updated quarterly
  - Some form of pattern matching



- Company's website suggests one signature will not detect other new devices if fundamental frequency is different
- Asked to participate in Black Dart 2014

Orelia

Sandia National Laboratories

- Company attributes:
  - Small French company founded in 2007
  - Claim to be experts in audio pattern recognition, machine learning, and signal processing
- Drone Detector:
  - Microphone detection of “generic” **acoustic** signature generated by electric propeller UAVs (fixed or rotary wing)
  - Recommended use:
    - Installation on flat, sound-reflective surface 3 m (10 ft) high
    - Longer range when background noise floor is less than 40 dB
    - Ethernet cable connection for communication and power
    - Alarm also available from contact inside the module

CellAntenna

Sandia National Laboratories

- Company attributes:
  - Solutions to enhance or prohibit cell phone signals
  - Based in Coral Springs, FL with offices in Europe
  - Completed development of D3T system in January 2015
- D3T (Drone Detection and Defeat Technology)
  - **RF emission** of controller and video signals
  - Max range: 1-2 km (0.6-1.2 mi) standoff distance, 300 m (1000 ft)
  - Antennas deployed within and at the fence line form a “bubble” of protection, not affecting systems outside
    - “Does not interfere RF communication”
    - Scalable to cover large areas
  - Signal is processed to determine the type of flight control system
  - Electronic countermeasure capabilities:
    - Taking control of the target (full control, land suddenly, send back to origin, etc.)
    - Depriving accurate GPS data
    - Simultaneous deployment of multiple countermeasures
    - Other proprietary techniques

DDC

- Company attributes:
  - Domestic Drone Countermeasures (DDC) founded in 2013
  - Very small company in Oregon City, OR (website has Kickstarter link)
- Basic Drone Detection System
  - RF emission device network that triangulates unknown receivers within a mesh grid of sensors
  - Detection of RF transmitters in the range of 1 MHz – 6.8 GHz
  - Ignores manual list of known transmissions
  - Expandable coverage by adding sensor notes
  - Each node can detect within 50 ft in all directions

Missiles

Sandia National Laboratories

- NATO acknowledges that a missile can destroy an LSS target given adequate lock-on and stable tracking, but no (unclassified) data is provided to support the guidance and tracking requirements
- Potential risk for collateral damage draws serious concerns about the appropriateness of this effector type for use in security of urban or sensitive environments
- Command line of sight (CLOS) guidance systems
  - System tracks target and missile
  - Line of sight required throughout engagement
  - Performance against LSS threats depends on ability of ground-based tracking sensors
- IR seeker missiles
  - Locks on to warm elements of the target
  - Small, low-emission targets against complex backgrounds are difficult
- RF seeker missiles
  - Locks on to RF radiation
  - Concerns about the effectiveness against LSS targets due to the missile's reliance on Doppler filtering to extract low targets from ground clutter
- Semi-active laser (SAL) seeker missiles
  - Not yet applied to GBAD systems

Guns and Ammunition

Sandia National Laboratories

- NATO concludes that guns can be effective against LSS targets, particularly with airburst ammunition
  - Assumes well-established target track
  - Limitations for micro UAVs
- Suspected ammunition amounts required for a kill are undesirable for urban and high-consequence environments
- Types:
  - Machine guns (5.56-12.7 mm)
  - Cannon guns (20-57 mm)
  - Low fire rate guns (76 mm)
- Machine guns are deemed unsuitable due to poor accuracy and range performance
- Cannons are already used in GBAD systems but are only effective against LSS targets using airburst ammunition
  - Micro UAVs may require significant amounts of ammunition
- Low fire rate guns seem ineffective against LSS targets, particularly swam attacks

Laser Weapons

Sandia National Laboratories

- Lasers require direct line of sight
- Varying degrees of effectiveness
  - Increased confidence generally requires increased cost
  - Large upfront cost driven by the maximum operating range and the necessary power, but per engagement costs are much less
- Collateral damage is reduced (compared to other techniques) by precisely focusing the beam on the target
- NATO notes that several demonstrations have shown the ability to destroy in-flight UAVs with 10's of kilowatts at ranges greater than 2 km
- Environmental conditions (e.g. rain, snow, fog, etc.) can attenuate performance
  - Target must also withstand same environmental conditions
  - Limitations may be less severe in the likely short-range scenarios for LSS threats
- Low power lasers – either "dazzle" or destroy electro-optical sensors on target
  - Laser must be in camera's field of view and in the transmission band of the sensor
  - Increased power can disrupt or damage the sensor
  - Potential to defeat UAVs that use optics for flight control
- Pulsed, medium power – damage or destroy first optical surface
- High power – can defeat the target structure
  - Effectiveness depends on target construction, material, and range
  - An area of intense research

Electronic Counter Measures (ECM)

Sandia National Laboratories

- Transmit EM signals somewhere between 10 kHz and several GHz; power between several watts up to gigawatts
- Generally do not need precise target location or tracking
- ECM for LSS targets for interfering with any RF receiver
  - Data and command links
  - GPS
  - Mobile cellular
  - Avionics systems (e.g. altimeters)
  - AM/FM radio waves
- Goal is to prevent successful reception or transmission of data
  - Narrowband jamming (denying platform use of that spectrum)
  - More sophisticated spoofing
- Comms ECM can be like a cyber attack; may be too time intensive, especially for a swarm scenario
- GPS ECM is simple due to the weakness of the GPS signals
  - Protection techniques exist to amplify the satellites' signal
  - Spoofing is more effective but also more difficult
- Personal communication devices are susceptible to jamming but interference to nearby systems is likely
- High power microwave (HPM) and high power EM (HPEM) weapons
  - Temporary disruption to physical destruction of unprotected electronics
  - Effectiveness depends on many external factors (E field, frequency, target shielding)
  - Friendly systems also effected if unprotected
  - Operation range unknown; not known to be used in GBAD system

Low Power Lasers

Sandia National Laboratories

- Green Laser Optical Warner (GLOW) – Thales Group (UK)
  - Gun-mounted, intense green light to warn
  - Narrow (long range) or wide (short range) beam choice
    - Narrow beam diameter is 0.5 m at 50 m range
    - Wide beam will "fill a car window"
- CIRCM – BAE Systems
  - Integrated aircraft protection solution for infrared-guided threats
  - Lighter, more advanced version of the ATIRCM system
    - ATIRCM detects a missile, rejects false alarms, cues infrared jamming system to the missile location, and emits high-energy infrared beam to defeat the missile's IR seeker
- Vigilant Eagle – Raytheon
  - About 18 years since work began for airport missile defense
  - Illuminates missile body with EM energy tailored to divert the missile
  - 3 primary components
    - Distributed missile detect and track system (MDT) – pre-positioned grid of passive IR sensors mounted on cell phone towers or buildings to cover the required detection space
    - Command and control (C2) system – provides pointing commands and connects to airport security; determines missile launch point
    - Active electronically scanned array (AESA) – EM fields well within the OSHA standards

High Energy Laser (HEL)

- Rheinmetall is a German automotive parts supplier and military technology group
- Skyshield air defense system
  - Rheinmetall Live Laser Demonstration 2013
    - "Successful engagement of a swarm of jet-powered droned by a stationary Skyshield air defence system, whose effectiveness likewise relies on a HEL effector"[1] (targets flew into the target zone one after the other)
    - "Demonstrated a complete kill-chain capability against vertical take-off UAVs"[1]
    - A radar detects and identifies the targets, then the rough and fine tracking is performed by the HEL system
    - Range of demonstration not given
  - Max range: 3 km (1.9 mi)
  - Available effectors include 1kW, 5kW, 20kW, 30kW, and 50kW
  - Uses beam superimposing technology

[1] http://www.rheinmetall-defence.com/en/rheinmetall_defence/public_relations/themen_im_fokus/rheinmetall_hel_live_fire/index.php

CLOS Missile Systems

Sandia National Laboratories

- Crotale NG – 1990 – all-weather short-range anti-air missile
  - Used to intercept low-flight missiles and aircraft
  - Uses VT-1 missile: Mach = 3.5, 11 km range, 8 m kill-zone, 6 km ceiling
  - S-band pulse Doppler radar (20 km), Ku-band TWT tracking radar (30 km), thermal camera (19 km), daylight CCD camera (15 km)
- JERNAS– 1996 – export name for the Rapier Field Standard C air defense system by MBDA
  - Rapier mk2 missiles and launcher: Mach > 2.5, guidance system is automatic IR and radar CLOS
  - Dagger target acquisition and surveillance radar – multi-beam high resolution 3D radar supplied by BAE Systems Insyte. J-band, max detect >15 km, 5 km max elevation, more than 75 threats per second
  - Blindfire tracking radar – differentnial monopulse frequency agile radar by BAE Systems Insyte. F-band, max detect at 15 km
  - Rapier surveillance radar – bearing data downloaded to tracking radar and launcher. Surveillance radar confirms target is hostile usig Successor Identification Friend or Foe (SIFF) from Raytheon Systems Limited

IR Seeker Missiles

Sandia National Laboratories

- Stinger
  - Lightweight, portable, shoulder-launched
  - “Fire and forget”
- Mistral 2 – 1997, French
  - Giraffe AMB3D air defense radars by Saab Microwave Systems
  - Passive IR seeker uses indium aresnide detector array operating in the 3-5 um waveband, developed by SAT, now Safran
- PZR Grom – 1995, Polish
  - Flight speed of 650 m/s (Mach = 1.9 at sea level)
  - Infrared aiming sensor

RF Seeker Missiles

Sandia National Laboratories

- AIM-120 AMRAAM (NASAMS system) – Raytheon
  - Baseline weapon of the National Advanced Surface-to-Air Missile System (NASAMS)
  - Announced Feb 2015 development of the AMRAAM Extended Range missile for ground-based air defense
  - Active guidance, all-weather, beyond-visual-range
  - Able to switch between active radar homing to passive homing (homing on jamming signals from target)
- Common Anti-Air Modular Missile (CAMM) family
  - Developed by MBDA for the UK
  - Has not entered service yet
  - Active guidance, all-weather, can receive mid-course guidance via a datalink before active seeker takes over
  - Does not need separated tracking radars

SRC Backup Slide

Sandia National Laboratories

- LSTAR (V)2 and (V)3 surveillance radars
  - Complete systems; TRL 8/9
  - Max range: 40 km (V2) and 50 km (V3)
    - Target size unspecified
  - Provide 3D target location
  - Coverage:
    - Azimuth: 360˚
    - Elevation: 0 – 30˚
  - “Few false alarms in challenging clutter environments”
  - Applies to UAS (no size distinction)

DISTRIBUTION

Quantity	Mail Stop	Name	Organization
1	MS 1003	Jonathan Salton	6533
1	MS 1003	Daniel Small	6533
1	MS 1006	John Russel	6514
1	MS 1006	Matthew Erdman	6514
1	MS 0781	Gabriel Birch	6525


Sandia National Laboratories