AiMT

Advances in Military Technology
Vol. 13, No. 2 (**2018**), pp. 157-171
ISSN 1802-2308, eISSN 2533-4123
DOI 10.3849/aimt.01233

State of the Art and Problems of Defeat of Low, Slow and Small Unmanned Aerial Vehicles

A. Dudush*, V. Tyutyunnik, I. Trofymov,
S. Bortnovs'kiy and S. Bondarenko

Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine

The manuscript was received on 18 January 2018 and was accepted after revision for publication on 28 May 2018.

Abstract:

The article deals with one of the most intensively developing threats for civilian and military spheres – hostile use of Low, Slow and Small Unmanned Aerial Vehicles (LSS UAVs). The classification of the LSS UAVs is given. The existing threats of using LSS UAVs are divided into three categories. Special attention is paid to the third category of threats, the main feature of which is a high level of training of the operator. Main advantages and drawbacks of LSS UAVs are considered. It is determined that the best strategy is to employ a hierarchy of countermeasures including regulatory countermeasures (prevention, deterrence, denial), passive countermeasures (detection and interruption) and active countermeasures (destruction). State of the art and current problems of possible countermeasures are analysed. The most promising LSS UAVs' counteraction technologies are described. Most attention is paid to specialized sensors and modern active counteraction means, such as programmable air burst munition and high-energy laser systems.

Keywords:

Low, Slow and Small Unmanned Aerial Vehicles (LSS UAVs), LSS UAVs classification, threats categories of using LSS UAVs, advantages and weak sides of LSS UAVs, hierarchy of countermeasures

1. Introduction

Despite the original prerogative of using Unmanned Aerial Vehicles (UAVs) technologies – also known as drones – for solving military problems, they can nowadays be used in a wide range of areas of national economy, as well as in both commercial and private applications. "BI Intelligence" expects sales of drones to

* *Corresponding author: Antiaircraft Missile Troops Department, Kharkiv National Air Force University, Sums'ka st. 77/79, Kharkiv, Ukraine. Phone: +380 50 194 77 16, E-mail: dudush.a.s.hnups@meta.ua*

surpass $12 billion in 2021, which is up by a compound annual growth rate of 7.6 % from $8.5 billion in 2016 [1].

Small-sized commercial UAVs are one of the most intensively developing threats in both military and civil spheres of activity. The intensive development of the commercial market of UAVs opens wide access to this technology for private consumers, state and non-state actors, increases their cost-effectiveness together with expanding their opportunities and improving their performance. The development of small drones has been supported by the miniaturization and cost reduction of electronic components (microprocessors, sensors, batteries and wireless communication units).

There is currently a wide array of small UAV applications in the civilian world, and many more are envisioned for the future. The use of UAVs to transport civilian air cargoes could be a lucrative area in the future. Using swarms or multiple UAVs is projected to be a key area in future UAV development that will enable more effective Intelligence, Surveillance, and Reconnaissance (ISR) due to increased availability of multiple sensors during a mission.

Military have also increased their interest in small UAVs, which can be used for short-range reconnaissance tasks, for electronic warfare, for laser target designation for other weapon platforms or for carrying small bombs [2]. A special type of small military UAV is the so-called attack UAV. This type of UAV is fitted with a high-explosive warhead that is flown by an operator and then loiters over a target area using their onboard sensors to firstly identify and then attack a target.

The above mentioned factors served as a catalyst for the emergence of a new type of threat – Low, Slow and Small Unmanned Aerial Vehicles (LSS UAVs), which began to be widely used by militaries and non-state actors (terrorist, insurgent, criminal, corporate and activist threat groups) all over the world. The most dangerous threats of LSS UAVs use for terrorist purposes are their equipment with Chemical, Biological and Radiological (CBR) weapons, firearms or bombs to provide attacks on critical infrastructure facilities, crowded places and on important political figures.

Therefore, the actual tasks are systematization of LSS UAVs' qualities that can be used for effective counteract of this type of threats, as well as analysis of typical structures of existing LSS UAVs' counteraction complexes and highlighting the advantages and disadvantages of countermeasures implemented by them.

2. Particular Qualities of LSS UAVs

2.1. Definition and Classification of LSS UAVs

Unlike traditional air targets, LSS UAVs: 1) fly at low altitudes (< 4 km) which makes them easily hidden by complex terrain; 2) move at slow speeds (< 50 m/s) and can hover, which makes them difficult to differentiate from birds, bats, kites and balloons; 3) are small in size (< 20 kg) and built of poorly-radar-reflective materials, making them difficult to sense.

In order to categorize LSS UAVs for security purposes, define them based on their Maximum Take-Off Weight (MTOW) and the typical capabilities that are associated with each platform's type, as shown in Tab. 1 [3] and Fig. 1.

LSS UAV platforms typically fall into one of the following three types [4, 5]:

- Fixed-Wing (FW) UAVs, which refer to unmanned airplanes (with wings) that require a runway to take-off and land, or catapult launching;

- Rotary-Wing (RW) UAVs, also called rotorcraft UAVs or Vertical Take-Off and Landing (VTOL) UAVs, which have the advantages of hovering capability and high manoeuvrability. These capabilities are useful for many robotic missions, especially in civilian applications. A rotorcraft UAV may have different configurations, with main and tail rotors (conventional helicopter), coaxial rotors, tandem rotors, multi-rotors, etc.;
- Flapping-Wing (FlW) UAVs, which have flexible and/or morphing small wings inspired by birds and flying insects.

Each of these platform types has pros and cons [5], which can be used to create effective means of countermeasures. For example, FW aircraft are capable of fast and efficient flight, but typically cannot hover. Rotorcraft can hover and are highly manoeuvrable, but are generally less efficient in forward flight than FW UAVs. Neither FW UAVs nor RW UAVs scale down well – both in terms of the aerodynamics that govern flight and in the performance of the components that are necessary to generate propulsion.

For actuation, RW and propeller-driven FW drones generally use electromagnetic motors. Some FlW aircraft also use electromagnetic motors, but require a linkage mechanism to convert the rotary motion of the motor to the flapping motion of the wings. Most of the LSS UAVs may be constructed using conventional methods, such as additive and subtractive machining and 'nuts-and-bolts' assembly.

Tab. 1 LSS UAVs categories

Categories	MTOW [kg]	Type	Payload [kg]	Coverage [km]	Speed [km/h]	Endurance [h]	Altitude [km]
Nano	< 0.5	FlW, FW, RW	< 0.1	< 1.5	0…80	< 0.5	< 0.1
Micro	< 2	FlW, FW, RW	< 1	< 10	0…100	< 1.5	< 1.5
Mini Light	< 10	FW, RW	< 5	< 25	0…150	< 3	< 3
Mini Heavy	< 20	FW, RW	< 12	< 50	0…180	< 5	< 4

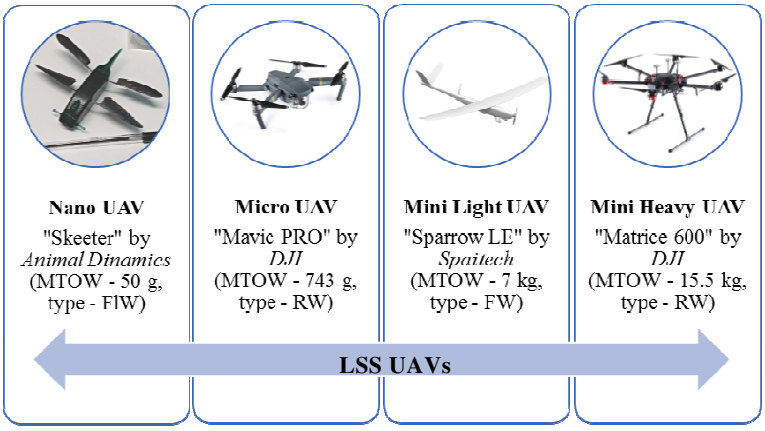

Fig. 1 Examples of LSS UAVs categories

2.2. Advantages of LSS UAVs

Numerous advantages presented by drone technology make LSS UAVs an attractive weapon choice for non-state actors' attacks, which poses serious security threats. The main advantages of LSS UAVs are [6, 7]:

- the possibility to attack targets that are difficult to reach by land (cars loaded with explosives or suicide terrorists);
- the possibility of carrying out a wide-scale (area) attack, particularly through the use of CBR agents or weapons in populated areas (even a small explosive device, delivered by a UAV to a place crowded by people, could inflict much more damage than the same device on the belt of a suicide terrorist);
- the covertness of attack preparation and flexibility in choice of a UAV launch site;
- the possibility of achieving a long-range and acceptable accuracy with relatively inexpensive and increasingly available technologies;
- the low operational altitude along with small size, small radar cross-section and small Infra-Red (IR) signature of the LSS UAVs makes it a difficult target for most of the common Ground-Based Air Defence (GBAD) systems, such as Surface-to-Air Missile Systems, Antiaircraft Guns and Shoulder-fired IR Missiles;
- the cost effectiveness of LSS UAVs compared with conventional UAVs and manned airplanes;
- the possibility of achieving a strong psychological effect by scaring people and putting pressure on politicians.

The most likely threats are Commercial Off-The-Shelf (COTS) and amateur LSS UAVs. This is due to a number of factors [6, 8]:

- the ability of obtaining the necessary knowledge, skills and equipment to make the UAV for "amateur aircraft modelling" almost out of control;
- the imperfection of the regulatory framework of using LSS UAVs both on the territory of states and over critical infrastructure objects;
- the development of goods delivery services using UAVs, which further complicates the problem of monitoring and identification of aircrafts, posing a potential threat.

2.3. Weak Sides of LSS UAVs

Like any aerodynamic aircraft equipped with a propulsion system and a set of radio electronic equipment, the LSS UAVs have certain limitations and a number of unmasking features.

The main weak sides of LSS UAVs are [3-7]:

- The poor weatherproofing. Most of COTS LSS UAVs have limited operating conditions. The ability to operate in a broader range of weather conditions, such as high winds, rain and snow, is specific for expensive COTS or military-grade drones. Weather resistance needs to add an extra weight for LSS UAVs. This would likely reduce flight time and payload capacity unless power or the number of rotors are increased.
- The poor resistance to external influences. Most of COTS LSS UAVs made of very lightweight materials like EPO foam, plywood, or plastics that have poor resistance to physical and temperature influences.

- The unmasking. In order to minimize mass of LSS UAVs, the platform electronics is relatively unprotected in terms of Electromagnetic (EM-) and IR-screening and the UAVs have Radio Frequency (RF) emissions that could be exploited by using narrow-band Electronic Signal Monitoring (ESM) systems. In addition, there is the potential for using acoustic to identify and classify LSS threats.

The basic unmasking signs of LSS UAVs' are:

a) EM emission of autopilot and navigation systems that might be feasible to undertake hostile missions without using any data-links;

b) RF emission of radio controlled transmission systems (e.g. command links, data links, communications) and sensors (e.g. altimeters, RF landing aids, radars);

c) IR emission of batteries and spinning rotor shafts;

d) acoustic emission of various drive-line components (e.g. electric motor, reduction gears and rotors etc.)

Hackers can also invade the main control system of the LSS UAVs, replacing the original users as the new drivers or controllers of the device. Malware script is loaded to the drone over a command link and can turn off the autopilot system and take control remotely.

- Jamming and hacking. To exclude the possibility of controlling UAV, drone control frequencies and Global Navigation Satellite Systems (GNSS) signals can be blocked around the target using a RF jammer. This removes the operator's ability to guide the UAV onto a target or to take evasive action against any active defence systems.
- Low level of technical reliability. The frequency of UAVs accidents is ten times higher than manned aircrafts. The main reasons for this are significantly less reliability of complex, "thin" radio electronic systems on board of the LSS UAVs and the complete lack of electronics reserves of the main systems due to their low carrying capacity.

3. Defeat of LSS UAVs

3.1. Threats of Using LSS UAVs

Non-state actors around the world have identified the two most dangerous categories of hostile use of LSS UAVs: attack and ISR.

Even without armaments, COTS drones are capable of causing damage or injury to people or vehicles on the ground or in the air. There are three known aircraft collisions and dozens of accidents and incidents, caused by UAVs around the world [9].

According to the study into the effects of a mid-air collision between LSS UAVs and manned aircrafts [10], 0.4-kilogram class MTOW quadcopter can penetrate birdstrike certified helicopter windscreens and critically damage tail rotors. Also it has been shown that mid-air collisions with 4-kilogram class quadcopter components and 3.5-kilogram class FW drones with exposed metallic components at high, but realistic speeds could critically damage airliner windscreens.

The most fearsome threat produced by non-state actors involves the deliberate construction or modification of UAVs to carry and employ weapons. A small explosive device, delivered by an UAV to a place crowded by people, could inflict

much more damage than the same device on the belt of a suicide terrorist. Therefore, there are particular concerns that LSS UAVs will be used as simple, affordable and effective airborne Improvised Explosive Devices (IEDs) [11].

First media reports of non-state actors' attempts to employ UAVs and to create airborne IEDs on their basis began to appear in the mid-nineties [6]. The main objects of attacks and the most vulnerable targets are critical infrastructure objects, places, crowded by people, and enemy equipment or troops.

In January 2017, the information about creating "Unmanned Aircraft of the Mujahideen" Islamic State's unit – a fleet of modified drones equipped with bombs to carry out attacks on enemy equipment and soldiers – has caused the greatest resonance. During the first week of using such UAVs, a number of successful attacks against Iraq Armed Forces were made and 39 Iraqi soldiers were killed or wounded [12].

Similar measures to equip the commercial UAVs with weapons are also undertaken by the Hezbollah and Hamas militants [13]. Hezbollah has released footage that supposedly shows its drones dropping bombs on Syrian rebel positions. Hamas has posted video and images of a drone in its possession that has four small rockets or missiles under its wings.

The ability to conduct persistent, low-cost ISR is a well-recognized and core advantage of LSS UAVs. The UAVs can collect targeting intelligence on adversaries' military assets to conduct kamikaze strikes or launch guided munitions if they were available. After initial strikes, drones can be used for battle damage assessment operations. In addition, LSS UAVs can capture and transmit propagandist video footage of attacks and messages from central leadership. In addition to the direct military benefits which drones have provided LSS UAVs can also be used for political effects: to publicly increase transparency, shape public opinion through propaganda, or sow misinformation [14].

For example, Jihadi groups fighting the Syrian government – most notably ISIS and Jabhet al-Nusra – are extensively using advanced drones to pinpoint the Syrian Army's locations, find out the information about troops deployment, and film suicide attacks and propaganda footages [12].

3.2. LSS UAVs Threats Classification

Civilian LSS UAVs are available as COTS Ready to Fly (RTF), Bind and Fly (BNF – with customizable transmitter) and Plug and Fly (PNF – with customizable transmitter, receiver, battery and charger) [11]. Users with no prior UAV flying experience can procure RTF models, and more experienced and knowledgeable users can purchase fully-customizable PNF models.

In order to analyse possible countermeasures, it is advisable to distinguish three categories of existing threats of using LSS UAVs [15]. The first one is the accidental unauthorized using of RTF UAVs, which might happen with either sophisticated or unsophisticated UAV operators. The second and the third categories are threats of deliberate unauthorized using of UAVs by unsophisticated and sophisticated operators respectively. The main feature of the third category of threats is a high level of training of the operator that can independently assemble PNF model using COTS or military technologies and finalizing its hardware and software tools for specific tasks.

One of the effective methods of counteracting the first and second categories of threats is the GNSS-enforced geo-fences within UAVs autopilot systems, when

manufacturers upload in the firmware of drones geodetic data about "no-fly zones" around airports, sports stadiums, Government buildings and other security-sensitive sites. When receiving data from the GNSS sensor about crossing boundaries of the "no-fly zone", the autopilot will automatically reject the trajectory of UAV from span above it or stop them at the boundary. As of 22 April 2017, the database of DJI company, one of the biggest manufacturer of commercial drones in the world, contains 7 824 "no-fly zones" around the world [16]. In addition, critical infrastructure facilities can be equipped with commercially available anti-UAV systems.

UAV intrusions of the third category of threats will be much more difficult to counter [15]. A sophisticated attacker could mount a kamikaze-style attack against a sensitive target using a FW powered glider with an explosive few-pound payload. The UAV glider could be launched tens of kilometres from the target. It could cut its engine on final approach to evade acoustic detectors, and it could be built of poorly-radar-reflective material (e.g. plywood) to evade radar detection. With only minor changes to the UAV's autopilot software, of which highly-capable open-source variants exist, an attacker could readily disable geo-fencing and could configure the UAV to operate under "radio silence", ignoring external radio control commands and emitting no radio signals of its own.

The UAV would thus be difficult to detect and would be impervious to command link jamming or hijacking. Moreover, the attacker could configure the autopilot to ignore GNSS signals during the final approach to the target, relying instead on an inexpensive magnetometer disciplined Inertial Navigation System (INS). Such a modification would render GNSS jamming or deception (spoofing) useless during final approach.

In light of the above, no single defence concept is completely effective at limiting the hostile use of LSS UAVs. The best strategy to counteract this threat is therefore to employ a hierarchy of countermeasures (Fig. 2) [11, 17].

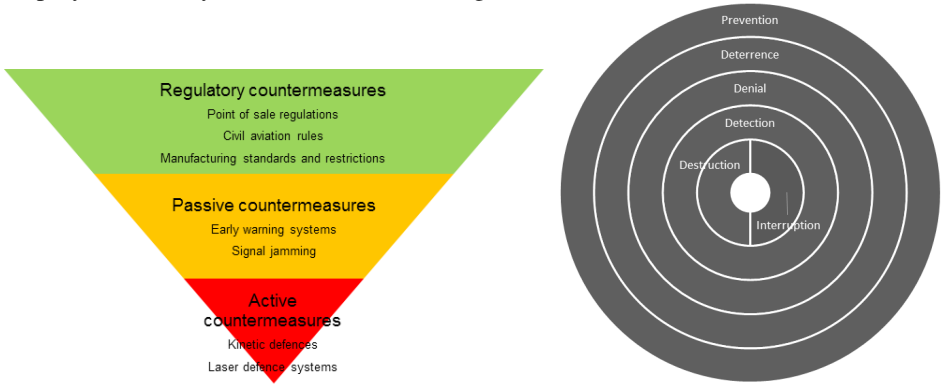

Fig. 2 UAV defence concepts:
left – Remote Control Project model [11]*; right –UAV Defence in Depth model* [17]

3.3. Regulatory Countermeasures (Prevention, Deterrence, Denial)

Domestic regulations can put in place a range of measures targeting on the control of full supply chain and life cycle of drones. Specific regulatory countermeasures may include [11, 17]:

- the procurement and import regulations, including mandatory registration for purchase and sale the UAVs above certain class (by flight range, payload, etc.);
- the civil aviation regulations on UAVs licensing and use, providing for administrative and criminal liability for flights near important state and critical infrastructure facilities;
- the firmware limitations, including "no-fly zones" and limiting MTOW and distance from the operator.

The main world regulator of the sales of delivery systems that can promote the dissemination of weapons of mass destruction (including the UAVs) is the voluntary Missile Technology Control Regime (MTCR) established in 1987. MTCR partners are 35 countries of the world. However, Israel and China, the biggest World manufacturers and exporters of UAVs, are not yet members of the MTCR. In addition, according to paragraphs 19.A.2 and 19.A.3 [18], licensing is required only for "complete unmanned aerial vehicle systems (including cruise missiles, target drones and reconnaissance drones) capable of a "range" equal to or greater than 300 km" or "equipped with or designed to carry an aerosol dispensing system/mechanism with a capacity exceeding 20 litres, and an autonomous flight control and navigation capability or the ability to sustain controlled flight beyond the line of sight of a human operator".

Therefore, nowadays the MTCR has goals that are more global while the problem of regulating the LSS UAVs sales is beyond the competence of this association and hence, it requires a relevant solution on the level of individual states or their unions.

The emerging UAV laws in Australia, Japan, the United Kingdom, USA and the European Union community offer different approaches that might be incorporated and adopted into national airspaces. Ten actions that have to be done for integrating UAVs into national airspaces over several years, are as follows [19]:

- to agree upon a concept of operations for UAV flight in civil airspace;
- to develop a classification scheme and definitions for UAVs as they relate to operations in civil airspace;
- to establish regulations for UAV system certification, flight operations, and ground controller qualifications;
- to develop effective technologies and procedures to prevent collisions of UAVs with other aircraft, the ground, or other obstacles;
- to institute security controls and approvals for UAV operations;
- to develop and implement communications solutions for UAV systems;
- to develop an aeronautical data exchange, processing, and synchronization network that accounts for unique UAV requirements;
- to harmonize UAV regulations, certification standards, and operational procedures;
- to ensure UAV interoperability with the air traffic system and to assess potential impacts on the air traffic system and its regulatory and operational environment;
- to gain public acceptance and active communication with all potential affected parties.

3.4. Passive Countermeasures (Detection and Interruption)

The complex of passive countermeasures includes detection and spatial coordinate measurement of the UAVs, recognition, identification of the UAV threats and RF

signal analysis for effective jamming of communication channels and command links or for interception of control.

Since the LSS UAVs belong to the class of low-observable aircraft and they have similar characteristics and parameters of the bird's movement, it seems to be necessary to use specialized detection and recognition systems. These systems may include both active and passive radars, ESM systems, acoustic and Electro Optical (EO) sensors. Wherein, the most effective solutions must integrate different types of the systems with Electronic Countermeasures (ECM) [3].

The main advantages of using active radars for detecting LSS UAVs are their ability to detect targets day and night in all-weather conditions and their independence from the presence of the own radio emission of targets. Despite the fact that the active radars are the main surveillance sensors of current Air Traffic Control (ATC) and GBAD systems, the using of conventional radars for LSS UAVs' detection is ineffective [3, 7, 20]. The main challenges for LSS UAVs detection using current high frequency sensors are the presence of false alarm plots and identification of real LSS threats that move with the same velocity as clutter or natural objects such as birds, "angels" or ground vehicles.

The world practice of solving this problem is to create specialized radars for LSS UAVs detection. The most suitable for these purposes are holographic (staring) radars [7, 21], whose design allows "looking" permanently everywhere in the wide transmission sector, but with a high angular resolution.

The outstanding features of such radars are their ability to detect:

- very fast and/or manoeuvring targets (including popping-up), thanks to their high update rate;
- very slow targets and/or non-stationary signature targets, thanks to their very high Doppler resolution;
- very small targets thanks to their long-term integration capacity.

These features make the holographic radars ideally suited for LSS UAVs detection. In addition to having a very low minimum detectable velocity, the fine Doppler resolution permits the detection of both the body motion and the internal motion of the target – sometimes referred to as "micro Doppler". In the case of a LSS UAV, the motion comes from the propeller which can give a unique indication as to the type of target being observed.

Clearly, this technique is unachievable in mechanically scanned surveillance radars or conventional phased array surveillance radars that can only afford to schedule short periods of time to a given sector in order to maintain complete coverage with acceptable latency.

The presence of electromagnetic radiation from the board equipment of the UAVs makes it possible to consider passive radars and ESM systems as an alternative to active radars.

The command links of the LSS UAVs generally occupy one of the three frequency bands reserved for radio-controlled devices (Tab. 2). Most frequently, the control and data transmission is carried out in the 2.4 GHz and 5.8 GHz band with the spreading of the signal spectrum by methods of Frequency-Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS), or using wireless communication protocols. Using phased arrays and the presence of parameters databases of the UAVs' control signals makes it possible to detect and recognize them for 10 μs to 500 ms after the signal interception [22].

Tab. 2 Main frequency bands for radio control channels of UAVs

Frequency band name	Low bound	High bound	Power restriction
UHF Short Range Device	433.05 MHz	434.79 MHz	≤ 10 mW ERP
2.4 GHz	2.4 GHz	2.4835 GHz	≤ 100 mW EIRP
5.8 GHz	5.725 GHz	5.85 GHz	≤ 100 mW EIRP

To increase the controlled area and to determine the spatial coordinates of the UAVs, multi-static passive radar systems (Passive Emitter Tracking – PET and Passive Coherent Location – PCL) can be applied which use Time Difference of Arrival (TDOA) localization technique. In this case, the possibility of co-processing the data, received in spaced positions, with their precise time synchronization should be realized [23].

Advantages of multi-static passive radar systems are the ability of determining the spatial coordinates of the UAVs and the operator, high reliability of recognition and determination type of the UAVs, preparation of the initial data for effective suppression of the command links and communication channels, as well as control interception of UAVs. However, when the third category of threats is being countered there is the risk of using the UAVs in the radio silence mode that can make it "invisible" for such systems.

Electric motors and engines of the UAVs produce specific sound that can be used for their detection and recognition by sound signatures. Acoustic sensors, even with the need to use systems of several sensors to determine the spatial object coordinates are an economically affordable alternative to radar.

Novel acoustic vector sensors capable of measuring acoustic particle velocity and pressure as in a standard microphone have a broad-banded detection capability from 0.1 Hz to 14 kHz with typically 1…2 degrees accuracy in the field. Acoustic vector sensors can localize various multiple acoustic sound sources simultaneously in 3D space [7].

Acoustic sensors can be quite effective in detecting kamikaze-style attacks due to the need for short-term operation of UAVs' propulsion units in the afterburner mode before they turn off while approaching the target. However, the small detection range of the LSS UAVs (up to 2 km) and the high probability of false alarms in the presence of external sounds similar to the operation of the UAVs (the operation of the electric trimmers, the reproduction of the UAVs flight recordings) now significantly limit their range of use [15].

To expand the capabilities of radars, ESM systems and acoustic sensors for detecting, recognizing and identifying the UAVs threats can be combined with passive or active EO sensors. Passive EO sensors operate over the Infra-Red (IR) section of the electromagnetic spectrum (0.75…1 000 μm). EO/IR sensors can detect the UAVs day and night by the thermal contrast of hot motors or batteries. The combination of IR cameras with thermal imagers and TV cameras enables to recognize and determine the type of LSS UAVs at distances up to 3 5000 m [24].

Active EO sensors or burst illumination LIDARs [25] have the working distance up to 10 km and an increased recognition and identification through bad weather effects including smoke, dust and fog. However, through narrow field of view for

a counter LSS UAVs application, they would benefit by being integrated with and cued on to target by complementary sensors such as radar, or passive EO/IR.

Detection, recognition and identification of the UAVs threats are the first stage of the passive countermeasures complex. The second stage is the selection of suitable method of protecting the object against a possible attack of the UAVs. For this purpose, passive countermeasures should provide the use of ECM systems for interruption of communication channels and command links of the UAVs ("soft kill capabilities").

The controlled flight of most of the LSS UAVs is carried out by means of two wireless communication links: command link and passive communication channel with GNSS. On this basis, the main task of the ECM equipment is to disrupt the communication links or to crack them and replace the information circulating in them.

Deception of the command links deprives the operator of the ability to control the flight of the UAV both in the Beyond Line-of-Sight (BLOS) mode, as in the First-Person-Viewer (FPV) mode. The result of jamming the command link of the UAV may be its fall, uncontrolled landing or activation of flight modes along the given route using GNSS data. To gain full control over the UAV and to carry out its controlled landing in a safe place, it is necessary to crack the command link. The latter is quite a difficult task if the controlling information is encrypted using cryptographic algorithms that are currently available even in the public domain.

The presence of the GNSS signals receiver in the onboard equipment of the UAV allows using an autonomous flight mode along the given route immediately after take-off. Therefore, an important element of the passive countermeasures complex is the deception of communication channel with GNSS. The civil codes of GNSS signals are open (unencrypted) and have low power, which makes it relatively easy to jam or to change the coordinate information.

The possibility of GNSS signal spoofing and flight path deviation of the UAVs is confirmed by theoretical and practical studies [26]. This technology can also be used for protecting area objects when choosing the appropriate system configuration and rational division of the protected area into sectors.

Deception of the communication links (command and GNSS) will make it practically impossible to use LSS UAV of the first and second threats categories. For the third threats category, allowing the use of commercially available INS in an autonomous mode will lead to significant deterioration in the accuracy of targeting the UAVs on the target. High accuracy INS and software used to provide highly accurate UAV navigation are very expensive and controlled by MTCR [18], and therefore they are unlikely to be used for organizing attacks of the third threat category.

At the same time, GNSS-deception and GNSS-spoofing systems also produce a serious threat to civil and military facilities using GNSS receivers (airfields, aviation, mobile and tactical communications). Therefore, using ECM is limited in the urbanized zone and must be strictly regulated.

However, GNSS information is not sufficiently precise for altitude regulation when flying a few meters above the ground and is not always available or reliable in confined areas, such as cities, forests and buildings. Therefore, autonomous LSS UAVs flying at low altitude will need more complex levels of control autonomy and additional sensors to detect distances from the surrounding environment and perform safe and stable trajectories. Vision is a promising sensor modality for small drones because, compared with other distance sensors such as sonar, infrared and laser range finders used in terrestrial vehicles, it does not require energy to interrogate the

environment, and for comparable mass, it can gather richer information and span wider fields of view [5]. This could be a new challenge for passive countermeasures.

3.5. Active Countermeasures (Destruction)

Despite the high efficiency of the complex using regulatory and passive countermeasures in countering LSS UAVs of the first and second categories of threats, there is still the possibility of overcoming them by threats of the third category. Therefore, in order to maximally protect important objects from the threats of using UAVs, the necessary condition is using the systems capable of destroying them ("hard kill capabilities"). The most effective systems of active counteraction of LSS UAVs include Programmable Air Burst Munition (PABM) and High Energy Laser (HEL) systems [7, 27, 28].

PABM is munitions which can be electronically programmed to detonate near the target at the ranges of up to 4 000 m. There exists two different PABM warheads, a sub-projectile warhead (kinetic energy) and a blast-fragmentation warhead (high explosives) with two fusing systems: time fuse and proximity fuse. The PABM effectiveness depends on the ability of the total system to place the ammunition close to the target within the lethal radius of the ammunition and the timing of the fusing.

With the sub-projectile warhead, the target is defeated by multiple impacts of heavy metal, spin-stabilized sub-projectiles. The sub-projectiles are released by precision programmable time fuse just in front of the attacking target. A short burst of the munition produces a dense cloud of lethal sub-projectiles covering the expected target position and penetrating the outer skin of the target, causing lethal damage to its interior.

The PABM technology is uniquely adjustable in many ways to allow optimal application for different missions and targets. This unique capacity for target and/or mission flexibility is characterized as follows [27]:

- The range of the payload release to the target can be adjusted in quasi-real time in relation to the size and vulnerability of the target to provide scalable lethality from deter to damage to destroy;
- The density and the number of sub-projectiles injected into the target plane can be varied by adjusting the gun burst length, rate of fire, and payload release point;
- The number and mass of the sub-projectiles can be optimized to counter specific threats and/or carry out different missions;
- There is growth potential to host alternative payloads e.g. decoys to be deployed precisely at ranges for specific roles.

Laser weapon has less destructive effects than PABM, but it can be quite effective in countering LSS UAVs in conjunction with ECM equipment providing disruption to the command links and communication channels with GNSS. There are three fundamental properties of a HEL [28]: firstly, the system is line-of-sight, requiring good visibility of the target; secondly, the time of flight is effectively nil; and finally, it delivers only thermal energy on the target's surface over a few to tens of seconds. Therefore, explosive substances and flammable surfaces of COTS LSS UAVs are an ideal target for such systems.

The high efficiency of using lasers for performing the combat tasks with LSS UAVs is due to the low cost of their use, the unlimited ammunition, the instantaneous

achievement of the target, the point impact on a specific target and the ability to control the radiation power depending on the application conditions and the required effect.

However, the need for continuous contact with the target over a period of time, as well as the possibility of using insulating, inflammable materials with a high melting point in the UAVs design can minimize the effectiveness of using HEL.

Nowadays active countermeasures are available mainly for military applications. Their use is justified only in cases when the prevented damage is commensurate with costs and risks, and the use of passive countermeasures is impossible or ineffective.

4. Conclusions

A wide range of benefits represented by drone technology makes LSS UAVs an attractive weapon choice for non-state actors' attacks, which poses serious security threats. There are two dangerous categories of hostile use of LSS UAVs: attack and ISR.

The most likely threats are commercial off-the-shelf and amateur LSS UAVs. Users with no prior UAV flying experience (first and second categories of threats) can procure Ready to Fly models, and more experienced and knowledgeable users (third category of threats) can purchase fully-customizable Plug and Fly models and upgrade hardware and software according to the concrete tasks.

Many advantages of LSS UAVs and analyses of study reports about different countermeasures conclude that no single defence concept is completely effective at limiting the hostile use of LSS UAVs by non-state actors. The best strategy is therefore to employ a hierarchy of countermeasures encompassing regulatory (prevention, deterrence, denial), passive (detection and interruption) and active (destruction) countermeasures.

Regulatory countermeasures, such as procurement and import regulations, civil aviation regulations on UAV licensing and use of firmware limitations, are aimed at the control of full supply chain and life cycle of drones.

The main weaknesses of LSS UAVs that can be used to passive and active countermeasures are poor weatherproofing, poor resistance to external influences, unmasking (EM, RF, IR and acoustic emission), jamming control frequencies and GNSS signals, hacking, and low level of technical reliability.

The first stage of passive countermeasures is detection, identification and identification of the UAV threats. Since current ATC and GBAD radars are not effective against LSS UAVs, conventional active radars must be integrated with acoustic or EO sensors that are not cost-effective. The most suitable approaches to LSS UAVs detection are multi-static active-passive radar systems and holographic/volumetric radars.

The second stage of passive countermeasures can include the use of ECM equipment of command links and communication channels with GNSS ("soft kill capabilities") for misdirection of the UAVs or interception of its control. However, LSS UAVs with a high degree of autonomy (third category of threats) still could remain dangerous and must be physically destroyed.

Modern active countermeasures must provide the usage of effectors ("hard kill capabilities") like Programmable Air Burst Munition and High Energy Laser.

For effective use of the "soft and hard kill capabilities", sensors must meet the following main requirements:

- To be capable of rapid detection and warning of LSS UAVs at military significant ranges with low false alarm rate.
- To guarantee high reliability of threat identification.
- To provide target designation that fulfils requirements of effectors.

References

[1] *Commercial Unmanned Aerial Vehicle Market Analysis – Industry Trends, Companies and What You Should Know* [on line]. BI Intelligence [cited 2017-12-01]. Available from: <http://www.businessinsider.com/commercial-uav-market-analysis-2017-8>.

[2] BAKER, B. *Small Bombs, Big Effect: Arming Small UAVs with Guided Weapons* [on line]. Air Force Technology [cited 2017-12-20]. Available from: <https://www.airforce-technology.com>.

[3] MUNDAY, R. *GBAD Sensor Mix Optimisation Study for Emerging Threats* [Study Report]. NATO: NIAG SG188, 2015, 237 p.

[4] VALAVANIS, K.P. and VACHTSEVANOS, G.J. *Handbook of Unmanned Aerial Vehicles*. London: Springer, 2015, 3022 p.

[5] FLOREANO, D. and WOOD, R.J. Science, Technology and the Future of Small Autonomous Drones. *Nature*, 2015, vol. 521, p. 460-466.

[6] MIASNIKOV, E. *Threat of Terrorism Using Unmanned Aerial Vehicles: Technical Aspects*. [Study Report]. Moscow: Moscow Institute of Physics and Technology, 2005, 26 p.

[7] MUNDAY, R. *Engagement of Low, Slow and Small Aerial Targets by GBAD* [Study Report]. NATO: NIAG SG170, 2013, 333 p.

[8] *Delivery Drone* [on line]. Wikipedia, the free encyclopedia [cited 2017-12-04]. Available from: <https://en.wikipedia.org/wiki/Delivery_drone>.

[9] *UAV-Related Events* [on line]. Wikipedia, the free encyclopedia [cited 2017-12-04]. Available from: <https://en.wikipedia.org/wiki/UAV-related_events>.

[10] *Small Remotely Piloted Aircraft Systems (drones) Mid-Air Collision Study*. [Study Report]. London: Crown copyright, 2016, 18 p.

[11] ABBOT, C. *Hostile Drones: the Hostile Use of Drones by Non-State Actors against British Targets* [Study Report]. London: Remote Control Project, 2016, 20 p.

[12] WARRICK, J. *Use of Weaponized Drones by ISIS Spurs Terrorism Fears* [on line]. The Washington post [cited 2017-02-21]. Available from: <https://www.washingtonpost.com>.

[13] *Non-State Actors with Drone Capabilities* [on line]. World of Drones [cited 2017-02-21]. Available from: <https://www.newamerica.org/in-depth/world-of-drones/5-non-state-actors-drone-capabilities/>.

[14] SANDER, A. *Game of Drones* [Wargame Report]. Washington: Center for a New American Security, 2016, 23 p.

[15] *Unmanned Aerial System Threats: Exploring Security Implications and Mitigation Technologies* [Hearing Report]. Washington: U.S. Government Publishing Office, 2015, 46 p.

[16] No Fly Zone Database as extracted 4/22/2017 from DJI Go4 apps [on line]. GitHub [cited 2017-05-01]. Available from: <https://github.com/MAVProxy User/ dji.nfzdb/blob/master/dji.nfzdb.csv>.

[17] WALLACE, R.J. and LOFFI, J.M. Examining Unmanned Aerial System Threats & Defenses: A Conceptual Analysis. *International Journal of Aviation, Aeronautics, and Aerospace*, 2015, vol. 2, no. 4, p. 1-33.

[18] *Missile Technology Control Regime (MTCR) Annex Handbook – 2017* [on line]. Brno: MTCR, 2017, 352 p. [cited 2017-12-11]. Available from: <http:// mtcr.info/wordpress/wp-content/uploads/2017/10/MTCR-Handbook-2017-INDE XED-FINAL-Digital.pdf>.

[19] RAVICH, T.M. The Integration of Unmanned Aerial Vehicles into the National Airspace. *North Dakota Law Review*, 2009, vol. 85, no. 597, p. 597-622.

[20] VISHNEVSKY, S. Potential Capabilities of Radiotechnical Troops Radars to Detect Operational-Tactical and Tactical Unmanned Air Vehicle (in Ukrainian). *Science and Technology of the Air Force of Ukraine*, 2017, vol. 2, no. 27, p. 92-98.

[21] HARMAN, S.A. and HUME A.L. Applications of Staring Surveillance Radars. In *Proceedings of IEEE International Radar Conference.* Arlington: IEEE, 2015, p. 270-273.

[22] HINDLE, P. Drone Detection and Location Systems. *Microwave journal* [on line]. June 2017. [cited 2017-06-15]. Available from: <http://www.microwave journal. com/articles/28459-drone-detection-and-location-systems>.

[23] SEDYSHEV, Y. and DUDUSH, A. Evaluation of the Impact of the Time Synchronization Accuracy of Multistatic Radar Positions on Errors in Determining the Spatial Coordinates of Aerial Objects. *Radioelectronics and Communications Systems*, 2013, vol. 56, no. 4, p. 178-185.

[24] WARNKE, H.W. Reconnaissance of LSS-UAS with Focus on EO-Sensors. In *NATO Military Sensing STO Meeting Proceedings (STO-MP-SET-241).* Canada: STO, 2017, p. 9-3-1–9-3-18.

[25] BAKER, I. and STORIE, K. Detector and Camera Technologies for 3D Active Infrared Imaging. In *NATO Military Sensing RTO Meeting Proceedings (RTO-MP-SET-130).* Orlando: RTO, 2008, p. 26-1–26-10.

[26] KERNS, A.J., SHEPARD, D.P., BHATTI, J.A. and HUMPHREYS, T.E. Unmanned Aircraft Capture and Control via GPS Spoofing. *Journal of Field Robotics*, 2014, vol. 31, no. 4, p. 617-636.

[27] *Oerlikon Ahead Air Burst Technology: Air Burst Munition (ABM)* [on line]. [cited 2017-06-15]. Available from: <http://en.calameo.com/books/ 005068186 ce3abb3008f7>.

[28] PUDO, D. and GALUGA, J. High Energy Laser Weapon Systems: Evolution, Analysis and Perspectives. *Canadian Military Journal*, 2017, vol. 17, no. 3, p. 53-60.