Explosive drones: How to deal with this new threat?

Geert De Cubber

Royal Military Academy (RMA), Brussels, Belgium

Abstract
As the commercial and recreative use of small unmanned aerial vehicles or drones is booming, so are the military and criminals starting to use these systems more and more. Due to improvements in flight stability, autonomy and payload capacity it becomes possible to equip these drones with explosive charges, making them threat agents where traditional response mechanisms have few answers against.
In this paper, we will discuss this new type of threat in detail, making the difference between the loitering munition, as used by regular armies and the traditional drones equipped with explosive charges, used in guerrilla warfare and by criminals. We will then discuss what research actions are currently being undertaken to provide answers to each of these threats and what countermeasures that are currently already available and which ones will be available in the near future.

1. Introduction

Recent advances in technology have rendered unmanned aerial systems (commonly referred to as drones) affordable, accessible and easily controllable by novice users. Together with the liberalization of the legal framework (which is still on-going), this has sparked the uptake of the technology for recreational use, but also for commercial use. Multiple good causes can also be referenced where drones are used for the benefit of the society, such as search and rescue [1] or humanitarian demining [2].

Unmanned aerial systems or drones are now becoming capable of navigating autonomously, even in tight spaces [3] and have become so small and agile that they virtually impossible to detect by classical detection methodologies for aerial threats (typically, RADAR installation installations). Moreover, these devices can be equipped with person detection [4] and even face recognition [5] software. Furthermore, as the drones become more and more capable to carry extended payload capabilities, it becomes possible to carry potentially hazardous payloads and to perform sophisticated attack operations, even with very cheap and commonly available drone platforms.

The enormous potential of unmanned aerial systems has unfortunately also already sparked the interest of malevolent individuals who use the technology for criminal or terrorist use [6], e.g. for terrorist attacks, activism, drugs and human trafficking, privacy invasion, etc.

In this paper, we will give an overview of the current existing threats, looking both into the popular commercially available mini drones as the military-type loitering munition and discuss what countermeasures are available to address these threats. The paper exclusively focuses on the threats related to small-scale systems (up to a few kg), so not the larger military systems.

2. Taxonomy of threats

2.1. Small rotorcraft drones used as attack vectors

Even though rotorcraft drones are immensely popular among the general public (and among criminals for spying and surveillance operations), their use as attack vectors for explosives is less widespread. This is due to several factors:

- Rotorcraft can only a limited (explosive) payload. Note that better system design, motors and battery systems will "solve" this problem in the future.
- Rotorcraft have a limited time of flight and range, meaning that the operator should not be too far from the target, which poses a problem in most circumstances (for the operator). Note that more autonomous capabilities and better battery technology will solve this "problem" in the future.
- Explosive charges carried as payload of a rotorcraft will on detonation explode in all directions, rendering the directed impact on the target smaller.

Notwithstanding these impediments, rotorcraft also provide some major advantages, such as their maneuverability in dense urban areas, their user friendliness and cost effectiveness. As a result, there have already quite some incidents:

- Already in 2016, the Islamic State used a drone with explosives to strike a Kurdish and French position in northern Iraq. The attack killed two Kurdish peshmerga fighters and wounded two French Special Operations troops.
- The first attempt to kill a political leader with an explosive rotorcraft drone was performed in 2018 by defectors on Venezuelan president Maduro during a speech he was giving to the Bolivarian National Guard's. Even though the attack failed, seven National Guard officers involved in the event were injured and treated in hospital. The attack was performed with a commercially available DJI M600 drone, customized to detonate a homemade bomb via the remote control.

2.2. Small fixed wing drones used as attack vectors

Fixed wing aircraft are able to cover long distances at great speed and loiter for long times monitoring their point of interest, which is an attractive proposition for operators of explosive drones that want to move themselves away from the action. Fortunately, there are also quite some disadvantages to the use of fixed wing drones to carry explosives:

- They are still quite expensive
- Handling a fixed wing drone requires much more skill and training than handling a rotorcraft drone
- They cannot hoover in place, which makes the precise delivery of explosive charges more difficult.

Noteworthy attacks with fixed wing drone systems are:

- In 2018, two explosive-laden fixed wing drones crashed in the yard of a governor's office's premises and a land belonging to the local gendarmerie headquarters in the Turkish province of Şırnak. The drones were laden with C-4 type explosives and were packed with nails and metal pieces to increase their impact.
- In 2017, a drone attack was performed in 2017 on an Ukrainian ammunition site. The drone dropped ZMG-1 thermite grenades. Although the fires were extinguished by Ukrainian servicemen, the incident still resulted in two deaths.

2.3. Loitering munition

Next to the malevolent use of drone technology by terrorists and criminals, also the military is more and more looking into the use of drone technology on the battlefield. Besides the regular and commonly known drones, the military also makes use of the so-called loitering munition. A loitering munition [7] is a type of unmanned aerial vehicle with and explosive warhead specifically designed to engage beyond line-of-sight ground targets. These types of drones are often equipped with high-resolution electro-optical and infrared cameras that enable the operator to locate, surveil, and guide the vehicle to the target. As such, they provide military units a quickly fieldable guided precision munition A defining characteristic of loitering munitions is the ability to "loiter" in the air for an extended period of time before striking, giving the operator time to decide when and what to strike

2.4 Swarm systems

Rotorcraft, fixed wing systems and loitering munition can be used as singular units. However, the real threat of drones as an attack vector comes when they are used in larger quantities for a combined and coordinated attack, as a so-called swarm. This is not science fiction; in 2018, a team of *ten* fixed wing drones with small rocket explosives attacked a Russian military base in Syria. No serious damage was reported, but it did show that a terrorist organization on the decline (ISIS) was still able to perform a coordinated attack. The United States unveiled in 2016 the Perdix program, where they are developing air-launched micro-drones that can fly in autonomous coordinated swarms. These small aerial vehicles can be programmed to autonomously detect and track objects, and could be armed for strike missions. Early trials were conducted with a coordinated flight of over 100 systems.

Future defensive counter-UAS systems will need to take into consideration the swarm aspect, as the relatively low cost of these tools will make it possible in the future for even guerilla organizations to organize such attacks.

3. Current research actions towards countermeasures

Within this section, we discuss some countermeasures that are being taken to address the threat of explosive drones. For addressing incoming threats posed by drones (equipped with explosive charges) a kill-chain has been developed by the USA Joint Chiefs of Staff, consisting of 6 steps, as depicted by Figure 1.

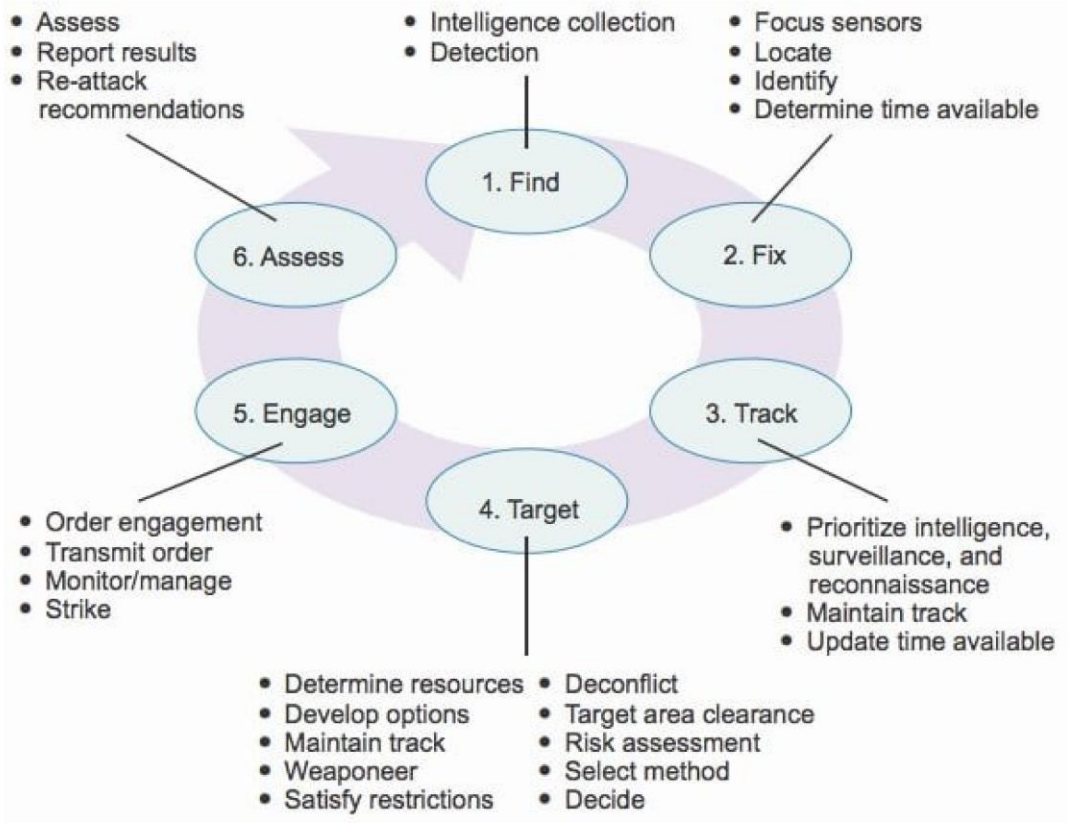

Figure 1. Kill chain for addressing drone threats (Joint Chiefs of Staff, 2013)

In this section, we will mostly focus on how technology can help in each of the different phases of the kill chain. We will discuss different response modalities, what they can do and to what types of threats they can pose an answer.

3.1. Non-proliferation

Whereas the explosives themselves are generally tied to export control regulations, such is not the case for most of the unmanned platforms that can be used as vectors for delivering the explosives. Indeed, mainly in the field of rotorcraft drones, there has been an explosion on the market of different types that are

commercially available and subject to no export regulation whatsoever. To a minor extent, this is true for the fixed wing models as well. Also here we see that terrorist groups like ISIS are using commercially available systems like the TALON drone for their operations.
Concerning loitering munition, there are obviously more restraints with respect to the wide availability of these systems. However, there are worldwide already a large amount of countries manufacturing loitering munition systems, so it is questionable whether it will be possible to constrain the technology from falling into the hands of the wrong people. Main producers of loitering munition include the United States of America, China, Russia and Israel, with also important production being performed by South Korea, the United Kingdom, Iran, Poland and Turkey.

3.2. Detection, Identification and Tracking by RADAR

What. RADAR systems able to detect drones are often derived from bird detection RADAR systems at airports and were then optimized for the detection of different types of drones.
Advantages. The advantages of RADAR systems are multiple: they work in all kind of weather conditions, provide a reasonable range (compared to other detection means) of a few kilometres and are capable to detect and track multiple targets.
Disadvantages. Major disadvantages of the RADAR systems are that they are still quite expensive and that this is an active system (emitting radio waves). It is therefore fairly easy for the adversary to detect the detector and to perform counter-countermeasures (e.g.; fly lower to avoid detection). While RADAR systems can provide some means of classification of targets, they mostly need a secondary sensor to provide a reliable classification.
Application to threats. As the RADAR systems can detect multiple targets, they are able to handle (small) swarms. In urban areas, the performance of the RADAR system will be reduced due to difficulty it has of dealing with the 3D structure of the terrain.

3.3. Detection and Tracking by 3D LIDAR

What. Comparable to the RADAR principle, 3D LIDARs use a focused light beam to search for aerial threat agents.
Advantages. The advantage delivered by the 3D LIDAR technology is that it is capable of performing a centimetre-precise localisation and tracking of the aerial threat agent (which is important for interception).
Disadvantages. The main disadvantage of the current 3D LIDAR technology is the relatively small range (less than a kilometre), which drastically reduces the intervention time. As LIDAR requires a line of sight to the target, it is also less reliable in urban environments.
Application to threats. The 3D LIDAR technology in its current state can be used as a complementary sensor to the RADAR (or other sensors, such as in the SafeShore project [8]), or can be used against slower moving targets in an open environment.

3.4. Detection and Identification by acoustics

What. Microphones can be used to pick up the sound of aerial threat agents. The more expensive types of microphones also allow to localize and track the treat agents and, in some cases, even to classify and identify them.
Advantages. An important advantage of acoustic sensors can be the relatively low cost and their capability to provide information on the type of threat agent approaching. Contrary to what may be believed acoustics detection can also work on both rotary *and* fixed wing drones, as the motors and rotors of the fixed wing drones do produce some noise in the (for us inaudible) ultrasonic domain.
Disadvantages. The main disadvantage of acoustic sensors is the very small range (much less than a kilometre), which drastically reduces the intervention time. As for the acoustic detector to work, the signal to noise ratio must be sufficient, this type of sensing methodology also has problems in noisy urban environments. The localisation and tracking capacity of acoustic sensors is far from ideal, as it is not evident to model the propagation of sound waves.
Application to threats. Acoustics sensors are mostly good for the detection and identification in not-too-noisy environments.

3.5. Detection, Identification and Tracking by Radio Frequency scanning

What. By scanning the frequencies used by the drones to communicate between the drone and the operator, these systems make it possible to detect and localize both the drone and the operator. [9]
Advantages. The advantages of radio frequency scanning systems are multiple: it is a totally passive system, they enable to localize the operator of the drone (which is really important, because arresting the operator of

an explosive drone is arguably the only safe way of bringing down the drone) and the range provided by some implementations of these systems is acceptable (a few kilometres).
Disadvantages. These sensors essentially scan for radio frequency emitters in the normal communication bands used. In an urban environment, where there are a lot of users of the communication spectrum, they have it therefore very difficult to single out the emissions due to drone communication.
Application to threats. Radio frequency scanning can work very well outside areas with a lot of radio emissions. More research is currently ongoing in order for the technology to operate reliably in areas with a lot of radio frequency emitters.

3.6. Detection, Identification and Tracking by cameras
What. Common daylight and infrared cameras equipped with threat agent detection software [10] and tracking software [11], enabling them to detect and follow threat agents.
Advantages. An advantage of these systems is that they enable not only to detect and track targets, but also to classify and identify them.
Disadvantages. The main disadvantage of cameras is that they cannot really be used for the first-time detection, as overlooking an entire airspace with cameras and performing detection on this data is beyond what is possible with the current state in sensor technology (lacking sensor resolution and sensitivity to look at far and close targets in one image, without zooming first) and computing technology (lacking processing power to process extreme high resolution video streams in real time). The cameras can therefore only be considered as secondary detection means for the identification and tracking. As cameras require a line of sight to the target, they are also less reliable in urban environments.
Application to threats. Cameras can be used for any type of threat agents but have difficulties with environments where the line of sight is not ensured. As they rely on other sensors for the detection and need to be pointed, they can only assess one target at a time, reducing their impact when confronted with swarms. They are also of great use for post-interception assessment.

3.7. Interception by Radio Frequency jamming
What. By flooding the communication spectrum the drone is using to communicate with its operator with white noise, it is hoped that the drone will fall back to a safe landing or return home operation.
Advantages. This is quite easy to do and quite easy to use.
Disadvantages. There are major dangers related to the interference with "friendly" radio frequency emissions that everybody is using nowadays. Therefore, these types of tools are often forbidden by national legislation for non-defence use. Obviously, autonomous drones are not affected by this interception methodology. Modern drones use advanced frequency-hopping techniques to ensure a reliable communication channel between the operator and the drone, so this technique is not becoming easier to implement.
Application to threats. Due to the considerations related to interference, the use in urban areas is problematic. Research is currently being performed concerning more directive targeted jamming systems, so this may evolve in the future.

3.8. Interception by GNSS jamming
What. By blocking the reception of the GNSS satellites signals (e.g. by flooding the frequency spectrum used), it is hoped that the drone will fall back to a safe landing or return home operation.
Advantages. This is quite easy to do. Would work on autonomous drones that use GNSS for navigation.
Disadvantages. There are major dangers related to the interference with "friendly" GNSS users.
Application to threats. Due to the considerations related to interference, the use in urban areas is problematic.

3.9. Interception by Radio Frequency spoofing
What. Hijacking the drone **by** taking over the telecommunication between the drone and the operator and send alternate control commands to the drone.
Advantages. Provides a safe way to land the explosive drone.
Disadvantages. Extremely difficult to perform for any type of drone. This is still a field of much research and full-fledged solutions that can perform radio frequency spoofing under realistic conditions haven't been proven on the terrain yet.
Application to threats. At the current technology readiness level, this technology hasn't been proven to be successful for an application terrain yet. However, potentially this is a very interesting research track.

3.10. Interception by GNSS spoofing

What. By creating a local alternate GNSS constellation, tricking the GNSS system of the drone into thinking it is elsewhere, hoping it will abandon the mission.

Advantages. This is certainly not impossible and provides a means to protect a critical infrastructure.

Disadvantages. There are major dangers related to the interference with "friendly" GNSS users. The explosive drone stays airborne and will likely after being re-routed just come back (or crash and explode elsewhere). There are more and more GNSS systems and modern drones combine their signals to improve their localisation accuracy, so this methodology is getting harder to implement.

Application to threats. Due to the considerations related to interference, the use in urban areas is problematic.

3.11. Interception by anti-aircraft guns

What. Traditional military anti-aircraft weapons, adapted to be able to intercept also drones.

Advantages. Able to intercept large and slow-moving drones from a reasonable distance.

Disadvantages. This system has many disadvantages for drones: obviously, it only be used outside urban areas, it is very expensive, it cannot be used at close range, it cannot be used for small fast-moving targets

Application to threats. Realistically, these tools can be used against single aerial threats posed by fixed wing systems that have a very predictable trajectory and a reasonably large surface area. Rotorcraft can often withstand a lot of damage before crashing and are less susceptible.

3.12. Interception by High Energy Laser

What. High-energy Laser fries incoming aerial threat agents.

Advantages. High-energy LASERs can very precisely target and destroy one drone from a reasonable distance (few kilometres)

Disadvantages. The cost for these systems is currently still extremely high. As a line-of sight methodology, it is less suited for urban areas.

Application to threats. At the current technology readiness level, this technology hasn't been proven to be cost effective on the terrain yet. However, there is a lot of research ongoing in this domain and a lot of potential for future improvements.

3.13. Interception by Electro-Magnetic Pulse Weapons

What. High-powered microwaves or electromagnetic pulses break down the electronics circuits of incoming explosive drones.

Advantages. As these weapons direct their energy in a wider area, they can be used against entire swarms.

Disadvantages. The cost for these systems if currently still extremely high and health issues for humans have not been sorted out. Their use in a civilian or urban context is therefore to be excluded.

Application to threats. At the current technology readiness level, this technology hasn't been proven to be cost effective and successful on the terrain yet. However, there is a lot of research ongoing in this domain and a lot of potential for future improvements.

3.14. Interception by birds of prey

What. Use specially trained birds (typically eagles) and learn them to "catch" drones.

Advantages. Relatively safe way to bring down an explosive drone (for the humans, not for the eagle).

Disadvantages. There are many disadvantages to this methodology: the training and maintenance costs are very high and the success is not guaranteed as the eagles are wild animals and not very responsive to human commands. There are also obvious objections with respect to animal welfare.

Application to threats. The Netherlands experimented with this methodology and stopped the program due to high operational costs related to training and maintenance.

3.15. Interception by nets

What. Launching a net (from the ground or from another drone) towards the incoming aerial threat agent in order to catch it and make it fall to the ground (or bring it down with a parachute).

Advantages. Man-portable ground systems now exist and the aerial solutions are getting more and more automated.

Disadvantages. There are many disadvantages related to this methodology: the range is extremely limited (a few dozens of meters), it requires a lot of training for the operator, it only works on slow-moving drones and in the end, the drone still crashes to the ground, which is very dangerous with an explosive drone.

Application to threats. Realistically, these type solutions are only applicable to cooperative targets that are slow moving close to the operator of the net-shooting device.

3.16. Interception by Kamikaze UAS

What. Use another drone to crash into the incoming drone.
Advantages. Solutions have been developed that are becoming more and more sophisticated and automated.
Disadvantages. The cost for these systems is still high and success is not guaranteed on faster targets.
Application to threats. Deploying these systems in a dense urban environment is probably not a feasible option, but they do provide a solution for soldiers, for protecting them against an incoming rotorcraft or fixed wing drone.

4. Conclusions

The conclusions of the discussions in the previous sections are summarized in Table 1, which shows for each of the discussed response mechanisms in what stage of the kill chain (corresponding to the definitions in Figure 1) can be provided for a specific threat agent and use case. As can be inferred from the table, there are no complete solutions yet to tackle all kinds of situations, certainly taken into consideration that not all solutions that are marked in green on the table have already reached the required level of technological readiness level (e.g. RF spoofing) or the required cost effectiveness (e.g. High Energy Laser) to make them believable options for the future. It is therefore certain that for the foreseeable future, a multi-faceted approach will be required, combining multiple detection and interception methodologies.
What is also clear is that more action is required into items related to the important 4th step of the kill chain: technologies to help the human decision maker prioritize, deconflict, perform risk assessment, and plan the resource allocation.
Finally, it will be paramount to further develop effective validation methodologies [12] for drone countermeasure systems, in order to come to clear standardized benchmarks of systems.

Table 1: Applicability of drone countermeasures within the kill chain

Threat agent \ C-UAS modality	1 Rotorcraft UAS – open area	1 Rotorcraft UAS – urban area	Fixed Wing UAS – open area	Fixed Wing UAS – urban area	Loitering Munition – open area	Loitering Munition – urban area	Rotorcraft UAS swarm – open area	Rotorcraft UAS swarm – urban area	Fixed Wing UAS swarm – open area	Fixed Wing UAS swarm – urban area	Loitering Munition swarm – open area	Loitering Munition swarm – urban area
RADAR	1,2,3	1,2,3	1,2,3	1,2,3	1,2,3	1,2,3	1,2,3	1,2,3	1,2,3	1,2,3	1,2,3	1,2,3
LIDAR	1,3						1,3					
Acoustics	1,2		1,2		1,2		1		1		1	
Radio Frequency scanning	1,2,3		1,2,3		1,2,3		1		1		1	
Cameras	2,3,6	2,3,6	2,3,6	2,3,6	2,3,6	2,3,6	2,3,6	2,6	2,6	2,6	2,6	2,6
RF jamming	5		5		5		5		5		5	
GNSS jamming	5		5		5		5		5		5	
RF spoofing	5	5	5	5								
GNSS spoofing	5		5		5		5		5		5	
Anti-aircraft guns			5		5							
High-Energy Laser	5		5		5							
EMP weapon	5		5		5		5		5		5	
Birds of prey	5											
Nets	5											
Kamikaze UAS	5		5									

green: satisfying level of performance; orange: certain performance, but not up to a satisfying level

References.

[1]. Geert De Cubber, Daniela Doroftei, Daniel Serrano, Keshav Chintamani, Rui Sabino, Stephane Ourevitch. 2013. “The EU-ICARUS project: developing assistive robotic tools for search and rescue operations”. IEEE international symposium on safety, security, and rescue robotics (SSRR). (October)

[2]. Yann Yvinec, Yvan Baudoin, Geert De Cubber, Manuel Armada, Lino Marques, Jean-Marc Desaulniers, Milan Bajic. 2012. “TIRAMISU: FP7-Project for an integrated toolbox in Humanitarian Demining”. GICHD Technology Workshop (September)

[3]. Olivier De Meyst, Thijs Goethals, Haris Balta, Geert De Cubber, Robby Haelterman, Autonomous guidance for a UAS along a staircase, International Symposium on Visual Computing, 466-475, 2015

[4]. Ichraf Lahouli, Evangelos Karakasis, Robby Haelterman, Zied Chtourou, Geert De Cubber, Antonios Gasteratos, Rabah Attia, 'Hot spot method for pedestrian detection using saliency maps, discrete Chebyshev moments and support vector machine', IET Image Processing, 2018.

[5]. Moshe Greenshpan, Face recognition on drones: an insider’s view, Keesing Journal of Documents & Identity June 2018, 33-35

[6]. Marian Buric, Geert De Cubber, "Counter Remotely Piloted Aircraft Systems", MTA Review, Vol. 27, No. 1, Military Technical Academy Publishing House, June 2017

[7]. Dan Gettinger and Arthur Holland Michel, Loitering Munitions, Technical Report, Center for the Study of the Drone, 2017

[8]. Geert De Cubber, Ron Shalom, Angelo Coluccia, Octavia Borcan, Richard Chamrád, Tudor Radulescu, Ebroul Izquierdo, Zhelyasko Gagov,"The SafeShore system for the detection of threat agents in a maritime border environment", IARP Workshop on Risky Interventions and Environmental Surveillance, Les Bons Villers, Belgium, May 2017

[9]. Angelo Coluccia, Marian Ghenescu, Tomas Piatrik, Geert De Cubber, Arne Schumann, Lars Sommer, Johannes Klatte, Tobias Schuchert, Juergen Beyerer, Mohammad Farhadi, Ruhallah Amandi, Cemal Aker, Sinan Kalkan, Muhammad Saqib, Nabin Sharma, Sultan Daud, Michael Blumenstein, Drone-vs-Bird detection challenge at IEEE AVSS2017, 14th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS 2017), Lecce, Italy, August 2017

[10]. Sanjoy Basak and Bart Scheers. Passive radio system for real-time drone detection and doA estimation. In 2018 International Conference on Military Communications and Information Systems (ICMCIS), pages 1-6, May 2018.

[11]. Geert De Cubber, Sid Ahmed Berrabah and Hichem Sahli, Colour-Based Visual Servoing Under Varying Illumination Conditions, Robotics and Autonomous Systems, vol.47, n. 4, pp.225 - 249, 2004.

[12]. Daniela Doroftei, Geert De Cubber, Qualitative and quantitative validation of drone detection systems, International Symposium on Measurement and Control in Robotics ISMCR2018, September 2018,Mons, Belgium