THE EXISTING TECHNOLOGIES ON ANTI-DRONE SYSTEMS

Laurențiu-Răducu POPESCU

"Carol I" National Defense University, Bucharest, Romania
lpopescu2011@gmail.com

Abstract: *The paper presents the technologies currently available on the market in the field of anti-drone systems (C-RPAS -Counter Remotely Piloted Aircraft System). These include technologies with the help of radar, audio interception systems or via infrared and electro-optical devices, which are limited in remote sensing. The purpose of this paper was to highlight the multitude of factors that can influence the main mission of C-RPAS systems, the detection. Without detection the other features of a C-RPAS system could not be applied. I used specialized documents and studies, but also comparative analysis as research methods. The results of the study confirmed to me the hypothesis that anti-drone systems use in combination, one or more of the technologies (to detect, to recognize, to identify, to locate, to block, to capture or to destroy the drone). The first four (the detection, the recognition, the identification, the localization) are in the basic configuration for any C-RPAS system. In the future, there will be a challenge (for the producers of C-RPAS systems), the capture of the RPAS, especially the military ones. It is also important to prepare the operators / beneficiaries for such systems. They can influence the effectiveness of drone combat missions.*

Keywords: RPAS, C-UAS, UAS, UAV, C-RPAS

1. Introduction

Starting from the definition of an anti-drone system (C-RPAS- Counter Remotely Piloted Aircraft System - anti-drone system) I will continue to present technologies that are currently on the market in this field, their strengths and weaknesses. A C-RPAS system represents a set of several technologies, for the detection, recognition, identification, localization, blocking, capture or destruction of the drone (RPAS- Remotely Piloted Aircraft System - the new name of the UAVs in the ICAO documentation).

- The Detection - consists of the detection of the RPAS, when it enters the operating area of the C-RPAS through radar, audio interception systems, motion sensors infrared and electro-optical devices;
- The Recognition - the ability of the C-

RPAS system to establish the distinctive signs of a specific feature of an RPAS, from a recognized aerial image of the system and to fit it into a defined class / category (for example Class I / mini RPAS, Class II / Tactically, Class III / HALE- High Altitude Long Endurance);

- The Identification - the ability of the C-RPAS system to detect from a recognized aerial image, several RPAS-specific features and to accurately recognize the model from a database (for example DJI Phantom 4, Shadow 600, RQ / MQ-1 Predator, RQ-8A Firescout, MQ-9 Reaper, Orion E, CH-5, IAI Heron, etc.);
- The Localization - the ability of the system to determine the precise coordinates of the RPAS in relation to the C-RPAS system;
- The Blocking - the ability of the C-

RPAS system to interrupt / annihilate the radio link (RFJ- Radio Frequency Jamming) between the flight vector (the aircraft itself) and the remote pilot or satellite link (GNSSJ- GPS or GLONASS Jamming) of the flight vector. When the radio connection is lost, the aircraft will either land or enter the RTB- Return To Base mode. The annihilation can also be achieved by “blinding” the electro-optical equipment or other research devices (radar with synthetic aperture, etc.) from the drone, using the LASER. High intensity microwave energy pulses are also used to annihilate the electronic components on board the flight vector;

- The Capture - the ability of the C-RPAS system to catch the flight vector using nets or other methods (handling protocol or "spoofing"). These nets are launched either from the ground or from the air, through another friendly drone;
- The Destruction - the ability of the C-RPAS system to destroy the flight vector through explosive charges, with the help of the LASER or other drones, which collide with the unauthorized drone. The LASER engages the aircraft using energy directed at certain vital components of it, destroying them.

Anti-drone systems use in combination one or more of the technologies listed above, the first four (detection, recognition, identification and localization) being in the basic configuration for any C-RPAS system. The effective combat method of drone makes the difference between the C-RPAS type systems existing on the market and here I refer to blocking / capturing / destroying the drone. For a better argumentation, study the paper “COUNTER-DRONE SYSTEMS” [1], published in December 2019. The ray detection of C-RPAS, based on radar, audio, video and radio frequency (RF) technologies are presented in the Table 1. Anti-drone technologies.

C-RPAS systems can have the platform (on which these technologies are mounted)

fixed, most often, or mobile (on various vectors such as automobiles or fighting machines, armored, ships or aircraft). There is also the slightly portable version (of the manipulation by one person), the C-RPAS system being operated by hand (similar to a rifle or small weapon).

Of course, first of all, detection is not an easy mission for C-RPAS systems, due to:

- The small dimensions and the specific shape of the RPAS, which must be combated;
- Special materials (anti-reflex-stealth technology) of the RPAS;
- Flight maneuvers at very low altitudes or in the urban area of the RPAS;
- Extremely low noise fingerprint electric motors of the RPAS;
- Fingerprint reduction devices in the visible and infrared spectrum of the RPAS composition;
- The frequencies used, the jamming and electronic warfare systems used.

For this reason, technologies with the help of radar, audio interception systems or through infrared and electro-optical devices are limited in distance and height. Next, I will detail these aspects and their influence on detection.

2. The Influence of the Specific Dimensions and Shape of the RPAS on the Detection

Depending on the class from which the RPAS comes from, the dimensions are different, starting from microdrones, small and even extremely small dimensions (see Figure 1 Microdrone Atom 1.0 (a), Nano QX (b), King King ET85 (c)) and to drones with dimensions comparable to modern transport aircraft (Global Hawk RPAS model) which is comparable to the U2 and Boeing 737 aircraft (see Figure 2 The comparable aircraft models regarding the bearing surface a.U-2, b. Boeing 737, c. RQ 4 Global Hawk).

Due to this diversity (regarding RPAS sizing) the radar detection is different. It is known that the reflected energy is directly

proportional to the size of the target (its reflection surface). In other words, the smaller the reflection surface, the smaller the reflected signal. The detection distance is influenced by this feature. In other words, if the drone is at a considerable distance from the C-RPAS and is also of small size, it is almost impossible to detect. The specific form of the RPAS is also important because it influences the amplitude of reflection of the signal emitted by the C-RPAS radar. Therefore, for effective

coverage of C-RPAS radar detection, motion sensors or various other sensors (MASINT-Measurement and Signature Intelligence) must be located. MASINT is a discipline that appeared after 1986, which identifies different types of machines, according to the static or dynamic technical characteristics. It was created for technical espionage, monitoring and control of weapons, environmental studies, etc. Includes acoustic, radar, laser, seismic, flow, flood, etc. sensors [3].

Table 1 Anti-drone technologies [8]

Surveillance technology	Drone signature	Localization/Tracking method	Detection range	Challenges
Radar	Micro Doppler	Doppler-based tracking delay-based localization	< 3000 m	low radar cross section
Audio	time-frequency feature	DOA-based localization	40-300 m	low speed and altitude
Video	appearance feature	motion- based tracking	100-1000 m	high ambient noise
RF	motion feature	RSS/DOA- based localization	< 1000 m	occlusion

(a) Microdrone Atom 1.0
Source: eBay.com

(b) Nano QX
Source: Amazon.com

(c) King King ET85
Source: Geekbuying.com

(a) U-2
Source: Airlinegeeks.com

(b) Boeing 737
Source: Cnet.com

(c) RQ 4 Global Hawk
Source: Defpost.com

Figure 2: The comparable aircraft models regarding the bearing surface

3. The Influence of Special Materials (Anti-Reflex-Stealth Technology) of RPAS on Detection

The radio waves are reflected differently. Therefore, the C-RPAS system must have a database with the signatures of the various RPAS (MASINT type). This database is done in time. Some RPAS producers are not interested in working together to build this database in the military production segment. And it is normal to offer their products to a larger segment of the market. In the civil segment, things are different. These RPAS producers are interested in selling to the general public as many drones as possible, especially of First Class, not encouraging the illegal use of civilian drones. That is why they will be interested in providing support to C-RPAS manufacturers in identifying different types of drones.

There have been realized specialized studies on detection. Following the studies done with multi-static radars, acceptable results have been obtained regarding drone tracking. For example, for the DJI Phantom 2 RPAS model, the radar did not exceed the detection distance of 3,000 meters. The example is useful to point out that, depending on the size and the materials used, the detection signal varies. In order to build a security architecture, in the case of strictly protected areas (objectives from the critical infrastructure of a state), several types of radar, with different operational (detection) radii, must be integrated. They must operate day and night under all weather conditions. For the protection of the population, high-power radars cannot be installed in urban areas, even if the protected objective is there. So, we have a big problem in these urban areas, at least in the case of long distance RPAS detection.

The radar emits a signal to the target, which turns into an echo signal. Following the obtained echo signal, the target image is formed, consisting of pixels whose "brightness" is proportional to the energy reflected by the target. The degree of

reflection is measured in decibels (dB). It is important to know that the echo signal of the natural surfaces, varies between + 5 dB (the brightest) and -40 dB (the darkest).

The echo signal depends on the following factors:

- The nature and orientation of the reflection surface;
- The degree of humidity of the reflection surface (the wetter the target, the more the reflected signal is stronger);
- The polarization of impulses;
- The relative angle of the antenna;
- The radar frequency.

The differences in structure of the reflection surface (in our case drone) and its orientation, are among the factors that influence the reflected energy towards the transmitter, resulting in the intensity of each pixel of the images formed on the radar monitor. To further complicate matters, for the army, Stealth technology RPAS is produced, which makes the C-RPAS detection distance considerably reduced. Of course, this technology encompasses several features, including: special absorbent paint, composition of materials from which RPAS is made, the shape of its reflection surface, on-board systems that reduce infrared radiation from drone engines and not lastly, measures to reduce the noise of its engines (for example RPAS type X-45, X-47, NEURON, etc.).

4. The Influence of Flight Maneuvers at Very Low Altitudes or in the Urban Area on the Detection

It is well known that in the urban environment, electromagnetic waves are influenced by the multitude of obstacles interposed between the emission source and the receiver. Moreover, the lower the target flies, the weaker the reflected electromagnetic waves. In our case, the source of emission is C-RPAS, and the receiver (target) is even the RPAS flight vector. The reflected signal depends on the arrangement and the materials from which the obstacles are built. If the remote pilot of

the RPAS will be sufficiently trained to operate through these obstacles, it may greatly reduce the vulnerability of the flight vector. It is well known that in the urban environment, electromagnetic waves are influenced by the multitude of obstacles interposed between the emission source and the receiver. Moreover, the lower the target flies, the weaker the reflected electromagnetic waves. In our case, the source of emission is C-RPAS, and the receiver (target) is even the RPAS flight vector. The reflected signal depends on the arrangement and the materials from which the obstacles are built. If the remote pilot of the RPAS will be sufficiently trained to operate through these obstacles, it may greatly reduce the vulnerability of the flight vector.

In conclusion, the C-RPAS detection, or better said the C-RPAS detection radii, may suffer variations in the urban area, depending on the C-RPAS and RPAS positions at a given time.

5. The Influence of Extremely Low Noise Fingerprint Electric RPAS Motors on Detection

C-RPAS systems use audio detection systems, such as acoustic sensors, to detect, classify and locate the drone. The sounds generated by drone engines are at different frequencies, depending on the type of motor used by the drones. Drones with electric motors have an extremely low noise footprint (due to the rapid rotation of the propellers, their shape and size, and their motor / engine model), especially when the distance from C-RPAS to RPAS is a little higher. In addition, there is noise in the environment, which does not help at all in selecting the sound signal produced by the drone (compared to the sound signal of the environment in which it evolves). In other words, the C-RPAS sound surveillance sensors are sensitive, both to the noise produced by the environment and to the typical noise of the drone, to the characteristic sound produced by its engines. In order to support the analysis, algorithms for processing acoustic signals are used, both in

time and frequency domains.

Christnacher et al. studied the acoustic signal coming from various mini-drones, using a network of tetrahedron acoustic panels. Following the measurements, it turned out that the C-RPAS sensors can detect the Quadcopter Blade 350 QX [4] drone (see Figure 3: Quadcopter Blade 350 QX), up to a distance of 150 meters, and for the DJI Phantom 2 model [5] (see Figure 4: DJI Phantom 2), up to a distance of 300 meters. These distances are very small, if we also take into account the speeds of these RPAS.

Figure 3: Quadcopter Blade 350 QX

Source: Mydronelab.com

Figure 4: DJI Phantom 2

Source: Amazon.com

Moreover, electric motors do not produce as much noise as classic piston engines or turboprop engines. That is why it is a disadvantage in terms of the detection distance of C-RPAS, the electric motors used on drones.

6. The Influence of Fingerprint Mitigation Devices on Visible and Infrared Spectrum from RPAS Structure on Detection

In the C-RPAS structure, there are electro-optical (EO) and infrared systems for video

detection and RPAS recognition. A drone can be detected based on specific features such as color, contour lines, geometric shapes [6] or edges and other movement characteristics [7]. There are drones that simulate the flight of birds (Ornithoptera- According to DEX (explanatory dictionary), Ornithopter - Aircraft heavier than air, with flying wings, which mimics the flight of birds). This makes it difficult for video analysis and especially for C-RPAS to recognize RPAS. There are currently methods that make it possible to separate the signal emitted by a flock of birds from a group of RPAS, either Ornithoptera. The experience of the C-RPAS operator in distinguishing the movement of birds is also important. The multifunctional EO systems from C-RPAS structure, based on the new generation of FLIR- Forward Looking Infra Red systems, play an important role. The sensitivity of these devices is quite good. For example, a target that has the size of a truck from a distance of 7.5 km can be recognized. An RPAS can be smaller or larger than a truck. “Depending on the size, targets can be detected at a distance of 20 km (for FLIR systems working in the 3-5 μ m band). On the EO system you can also mount improved FLIR equipment (8-12 μ m) with GPS link and laser light targeting pointer, which performs video tracking and programmable graphic representation for the targets” [8].

As can be seen in Table 2 Infrared wavelengths, the devices that work in the 3-5 μ m band are those that work with electromagnetic waves in the Near Infrared, and the advanced ones in the 8-12 μ m band, are the ones that work with electromagnetic waves in the Middle Infrared. C-RPAS FLIR detection can distinguish between a flock of birds (with a certain caloric radiation) and a group of RPAS (with a different caloric radiation).

Table 2. Infrared wavelengths [9]

The wavelength name (λ)	Limits λ
Far Infrared	420 – 100 μ m
Middle Infrared	100 – 10 μ m
Near Infrared	10 – 1,76 μ m

The delimitation of the RPAS is due to their temperature difference from the surface of the environment.[10] There are environmental influences that can affect the infrared detection. For example, detection in the direction of the sunset or sunrise is avoided.

7. The Influence of Radio Frequency (RF) of RPAS on Detection

Two of the multiple issues identified by the JAPCC - Joint Air Power Competence Centre regarding the RPAS (Center of Excellence for NATO Air Power in Kalkar - Germany) were related to the frequency, namely that "there is not enough bandwidth to provide what is required for current UAS- Unmanned Aerial System - another name assigned to RPAS operations" and "there are no dedicated frequencies for UAS. There are no internationally standardized frequencies for UAS operations, as there are for pilot aircraft operations".

Starting from these aspects I want to emphasize the complexity related to radio frequency (RF) of a drone. If for civil RPAS encryption / security is not so necessary, for military ones it is a mandatory condition, as protection systems for encryption keys are required, therefore the existence of communication protocols. This encryption must be operational, both for the command-control system, the RPAS flight platform, and for the signal captured by the payload sensors. For example, in Shadow 600 we have “Two-band communications, C-Band and UHF, using three channels:

- UPLINK - for the connection between

G.C.S and the plane, in the C-band, with the operational ray between 100 m and 200 km;

- UPLINK - for the connection between G.C.S and spare plane, with a lower frequency;
- DOWNLINK - the analogue link between the aircraft and G.C.S, used to transmit the collected information, both video and audio.”.[11]

Also, backup channels for datalink must be performed. Most often the military RPAS operates in frequency hopping. As a result, the C-RPAS detection of the working frequency of the RPAS is if not very difficult, I would say impossible. Some civilian RPAS (existing on the market) operate in specific frequency ranges (2,400-2,483GHz). But also, in the variants of civil mini-drones, the technology of frequency jump started to be implemented. For example, mention the DJI Phantom 4 model (see Figure 5: DJI Phantom 4), which operates in a frequency range between 5.725-5.825GHz, but also 2.4GHz for video transmissions.[12] So, we have a dual frequency transmission (OcuSync HD). This switching system is useful when there is strong signal interference, the system choosing in real time the optimal working frequency.

Figure 5. DJI Phantom 4

The problem of C-RPAS detection is complicated when the drones have the same frequency band as the Wi-Fi signal. A wide range of radio frequencies between 1MHz-6.8GHz [13] can be monitored, but that does not mean that any signal emission can come from a drone, which can generate false alarms from the C-RPAS system and

thus confusion for the operator of C-RPAS. Some military RPAS also have on-board jamming and electronic warfare equipment. These issues complicate things, both for the producers of RPAS, but also for those of C-RPAS. RPAS must have stable communications under jamming conditions, and the C-RPAS system must cope with jamming and electronic warfare equipment on board the RPAS. C-RPAS systems must be compatible / interoperable with national, NATO and EU structures to identify RPAS and friendly pilot aircraft operating in the vicinity of C-RPAS. That is why I believe that in the future, all aircraft, whether with or without pilot, regardless of their size, will have to be equipped with IFF-Identification, friend or foe systems.

Also, in the future, there will be a challenge (for the producers of C-RPAS systems), the capture of the RPAS, especially the military ones. Most RPAS have systems that anticipate operating errors and react accordingly. Thus, the remote operator / pilot of the RPAS must be warned of the loss of communications (transmission / reception), loss of GPS signal, low or critical battery voltage level, low altitude, engine failure, exit from the normal operating range of the system parameters / sensors on board the flight vector. The loss of communications (transmission / reception) and the loss of GPS signal are taken over by the RTB base return system existing on the RPAS, precisely to eliminate unplanned signal losses between the flight vector and the ground base. If the fault / signal loss has not been remedied, within a short period of time, the RPAS RTB system automatically enters this operating mode, with the flight vector returning to the base without any further commands. Even if some C-RPAS can enter the RPAS frequency, they are less likely to communicate with it or intervene in the RPAS flight. These C-RPAS capture systems are targeted more at civilian mini-drones who do not have additional protection systems.

8. Conclusions

There is a great diversity of elements and technologies that can and are used to combat RPAS. The main features of a C-RPAS system are those related to the detection, recognition, identification, localization, blocking, capture or destruction of the drone (RPAS). I sought to highlight the multitude of factors that can influence the main mission of C-RPAS systems, the detection. Without detection the other features of a C-RPAS system could not be applied.

As you can see, in the future there will be many challenges related to combating RPAS that C-RPAS producers will have to face. But what I want to point out is that the operators / beneficiaries of such systems can also influence the efficiency of drone

combat missions. In the evolution of weapons first appeared the weapon and then against its weapon, as the knowledge of the principles and technologies existing at that time. This process is present and ongoing even for drones. Conflicts and events in which RPAS and C-RPAS will be involved will determine the effectiveness of some or others over a certain period of time.

Finally, I must point out the security challenge, related to the illegal use of the RPAS, these systems making vulnerable even the most complex anti-aircraft defense systems known today. Therefore, the issue related to C-RPAS will be on the working table of producers and operators/beneficiaries around the world, constituting a current and future problem.

References List

- [1] A. H. Michel. COUNTER-DRONE SYSTEMS, 2nd Edition, Center for the Study of the Drone at Bard College, 2019, pp.18-42.
- [2] Xiufang Shi, Chaoqun Yang, Weige Xie, Chao Liang, Zhiguo Shi and Jiming Chen, Anti-Drone System with Multiple Surveillance Technologies: Architecture, Implementation, and Challenges [Internet]. Research Gate; Available from: https://www.researchgate.net/publication/324514116_Anti-Drone_System_with_Multiple_Surveillance_Technologies_Architecture_Implementation_and_Challenges
- [3] M. Axante- Research, Information, Espionage, Niculescu, 2005, p.196.
- [4] J. Brown, BLADE 350 QX QUADCOPTER: AN ADVANCED DRONE FOR MULTIPLE APPLICATIONS, [Internet]. MyDroneLab; Available from: <https://www.mydronelab.com/reviews/blade-350-qx-quadcopter.html>
- [5] F. Christnacher, et al., Optical and acoustical UAV detection, Proc. of SPIE Security+ Defence, vol. 9988, 2016, pp. 99880B-1–99880B-13.
- [6] Z. Zhang, Y. Cao, M. Ding, L. Zhuang, and W. Yao, An intruder detection algorithm for vision based sense and avoid system, Proc. IEEE ICUAS, Arlington, VA, USA, 2016, pp. 550–556.
- [7] S. R. Ganti, Y. Kim, Implementation of detection and tracking mechanism for small UAS, Proc. IEEE ICUAS, Arlington, VA, USA, 2016, pp. 1254–1260.
- [8] L.R. Popescu, The Use of Aerospace Systems Without Human Pilot on Board, The Publisher of The Carol I National Defense University, Bucharest, 2012, p.44.
- [9] E. Străinu, S. Topor, The Radio-Electronic War, Z2000 Publishing House, p.20.
- [10] L.R. Popescu, The Use of Aerospace Systems Without Human Pilot on Board, The Publisher of The Carol I National Defense University, Bucharest, 2012, p. 41.
- [11] L.R. Popescu (sole author), AIRCRAFT SYSTEMS WITHOUT HUMAN PILOT ON BOARD. General Considerations, Implications on Military Actions, The Publisher National Defense University, "Carol I", Bucharest, 2012, p. 244.

- [12] Phantom 4 [Internet]. Drona Romania; [n.a., 09/01/2020]. Available from: <https://www.dronaromania.ro/phantom-4-pro-v2-0/>
- [13] Domestic drone countermeasures, DDC; [n.a., 17/04/2017]. Available from: <http://www.ddcountermeasures.com/products.html>