Counter Remotely Piloted Aircraft Systems

Marian BURIC and Geert De CUBBER

***Abstract*—An effective Counter Remotely Aircraft System is a major objective of many researchers and industries entities. Their activity is strongly impelled by the operational requirements of the Law Enforcement Authorities and naturally follows both the course of the latest terrorist events and technological developments. The designing process of an effective Counter Remotely Aircraft System needs to benefit from a systemic approach, starting from the legal aspects, and ending with the technical ones. From a technical point of view, the system has to work according to the five "kill chain" model starting with the detection phase, going on with the classification, prioritization, tracking and neutralization of the targets and ending with the forensic phase.**

***Index Terms*—Counter Remotely Piloted Aircraft Systems, drone, drone detection tracking and neutralization, RPAS, SafeShore.**

I. Introduction

The general objective of this paper is to highlight the increasing requirement for an effective Counter Remotely Piloted Aircraft System[2] (C-RPAS) against malicious and terrorist use cases of Remotely Piloted Aircraft Systems (RPASs).

There is a continuous increasing of number of the RPASs applications in commercial and non-commercial fields (e.g., industry, agriculture, services, research, scientific, governmental non-military and so on) but unfortunately in the same time the RPASs have been becoming a really threat and weapon in present-day asymmetric warfare, terrorist attacks or malicious uses [1].

Mitigating the threats of illegal use of the RPASs envisages both legal and technological aspects. On the legislation side, the aim is RPAS integration into non-segregated airspace in multi-aircraft environment (including manned vehicles) [2]. On the other hand, the technological aspect aims to adapt and provide the technologies necessary to avoid mid-air collisions and to make RPAS technology compliant with national and international agreed aviation certification standards. In the same time, as a last radical solution it is imperious to design an effective counter RPASs according to an acknowledged standard.

The RPASs are used for civil or military goals. We have in mind in this work only RPASs which was designed to be used by civilians in recreational or commercial applications. There are many criteria for RPASs classification according to principle of flying and configuration, flight characteristic and handling, autonomy, endurance, kinetic energy, maximum weight or payload capacity, purpose and so on. In this paper, we take into account low, slow, small RPASs, fixed wing and rotary-blade RPASs, up to 20 kg MTOM, glider, quadcopter or jet turbine types (the last one is low, fast and small), according to European[3] and American classification [3].

In the second chapter, there is a brief inventory of the main risks which RPASs could bring if they are used in a malicious manner (e.g., as weapons, for intelligence, illegal traffic or smuggling) or inadequately use causing unintentional people injuring or even death.

The third chapter is the main one where there are shown the whole phases of a complete C-RPAS starting with detection and end up with forensic phase.

As a practical example, a special chapter was designed for SafeShore project[4] presentation. The mission of the SafeShore project is to tackle existing problems and gaps in coastal border, perimeters and objectives surveillance by developing a system for detection and tracking of RPASs using state-of-the-art, low cost, and low-emission technology.

II. Remotely Piloted Aircraft Systems as Weapons

Malicious uses of the RPASs

RPASs had been used until few years ago, only on military purposes. Now, RPASs with nearly same features and capabilities can be used for military, commercial and civilian purposes becoming dual use technology. It is very well known today that RPASs have recently joined to the other common things which can become suddenly lethal weapons [5].

Unfortunately, this emerging threat has not mitigated by appropriate legal, regulation and procedures specifically for dual use technology or through technical countermeasures. Moreover, if up to now this threat has been familiarly only in conflict zones, now it is moving towards the western world against civilians. It is becoming harder and harder to deal with export control as globalization is a very well-known phenomenon and China is manufacturing leader of the commercial RPASs.

It is obvious that the risks which these RPASs could represent must be carefully assessed and like in mostly any risk process assessment it is necessary to start with threats inventorying. Some of the most important threats are highlighted in Table I where for each threat is shown the RPASs category which is the most suitable and one or more footnotes to representative examples of use cases [1], [3-4],[6].

This work was supported in part by the European Union's Horizon 2020 research and innovation programme under grant agreement N°700643.

Marian Buric is with the Protection and Guard Service, Geniului Street, no. 42B, sector 6, 0600117, Bucharest, Romania (e-mail: buric.marian@spp.ro).

Geert De Cubber is with the Royal Military Academy of Belgium, 30, Av. De La Renaissance, 1000 Brussels, Belgium (e-mail: geert.decubber@rma.ac.be).

[2] A Remotely Piloted Aircraft System is composed from Remotely Piloted Aircraft (RPA) and associated Remotely Control Unit (RCU).

[3] www.ultraconsortium.eu

[4] www.safeshore.eu

TABLE I. RPAS ASSESSED AS THREATENING VECTORS

Threats	Appropriate RPAS type / classification
Violation of privacy[5]	Quadcopter ≤ 2 kg
Intelligence (ISTAR – information, surveillance, target acquire and reconnaissance)[6]	Quadcopter ≤ 2 kg Glider
Weapons and ammunition transport[7] [8]	Quadcopter ≤ 20 kg
Terrorist attacks using weapons, bombs, grenades, radioactive materials, etc.[9] [10]	Quadcopter ≤ 20 kg
Intentional collide with other authorized aircraft vehicles[11]	All quadcopter types Jet turbine
Using drones as projectiles (kamikaze drones)[15]	Jet turbine
Unintentional collide with other authorized aircraft vehicles[12] [13]	All quadcopter types Glider Jet turbine
People injuring [14]	All quadcopter types Jet turbine
Propaganda (looking for headlines)[15]	Quadcopter ≤ 2 kg
Critical infrastructure, properties and goods damage[16] [17]	All quadcopter types Jet turbine
Transport of the illegal objects (smugglers)[18]	Quadcopter ≤ 20 kg Glider
Stopping or slowing commercial RPASs' industry development[19] [20]	N/A

[5] http://www.quadcoptercloud.com/drones-invade-privacy/, accessed June 12, 2017

[6] Peter Bergen and Emily Schneider, "Now ISIS Has Drones? - CNN.com," accessed June 2, 2017, http://www.cnn.com/2014/08/24/opinion/bergen-schneider-drones-isis/

[7] Lizzie Dearden, "Revealed: Isis developing weaponized drones in secretive program", accessed June 12, 2017, http://www.independent.co.uk/news/world/middle-east/isis-weapons-drones-uav-programme-development-weaponised-explosives-surveillance-terrorist-groups-a7371491.html#gallery

[8] https://www.cnet.com/news/oh-look-a-drone-that-fires-a-gun/

[9] Michael S. Schmidt and Eric Schmitt, "Pentagon Confronts a New Threat From ISIS: Exploding Drones," The New York Times, October 11, 2016

[10] David Kravets, "Man Lands Drone Carrying Radioactive Sand on Japanese Prime Minister's Office," Ars Technica, accessed June 2, 2017, https://arstechnica.com/tech-policy/2015/04/manarrested-for-flying-drone-carrying-radioactive-sand-in-tokyo/

[11] Adam Rawnley, "So bad news: Now militants are using drones as projectiles", accessed June 2, 2017, https://www.wired.com/2017/04/bad-news-now-militants-using-drones-projectiles/

[12] Robert Pigott, "Heathrow plane in near miss with drone", accessed June 12, 2017, http://www.bbc.com/news/uk-30369701

[13] Luke Duecy, "Helicopter crew spots drone flying feet above KOMO chopper", accessed June 12, 2017, http://komonews.com/news/local/helicopter-crew-spots-drone-flying-feet-above-komo-chopper

[14] Martin Weil, "Drone crashes into Virginia bull run crowd", accessed June 12, 2017, https://www.washingtonpost.com/local/drone-crashes-into-virginia-bull-run-crowd/2013/08/26/424e0b9e-0e00-11e3-85b6-d27422650fd5_story.html

[15] John Hall, "Latest ISIS Video Shows Drone View of Kobane's Battle-Ravaged Streets of Kobane", accessed June 12, 2017, http://www.dailymail.co.uk/news/article-2871389/ISIS-propagandaCall-Duty-style-Latest-footage-shows-drone-s-view-battle-ravaged-streets-Kobane-swoopinggun-battles-ground.html

[16] Dan Shea, Amanda Essex, Ben Husch, "Drones and critical infrastructure", accessed June 12, 2017, http://www.ncsl.org/research/energy/drones-and-critical-infrastructure.aspx

[17] Dr Graeme Anderson and Andrew Chadwick from Frazer-Nash, "Protecting critical infrastructure from drones: managing the risks", accessed June 12, 2017, https://www.theengineer.co.uk/protecting-critical-infrastructure-from-drones-managing-the-risks/

[18] Ashitha Nagesh, "Drones used by gangs to fly illegal drugs into prisons", accessed June 2, 2017, http://metro.co.uk/2015/09/17/drones-used-by-gangs-to-fly-illegal-drugs-into-prisons-5395305/

[19] Commercial RPASs sector development is predicted to be worth $2 billion by 2020, according to B.I. Intelligence market forecasts

Vulnerabilities on RPASs using

Once the threats have been evaluated, the next step consists on vulnerabilities analysis. Each threat is focusing on at least one vulnerability. Therefore, it is important to briefly highlight some of these vulnerabilities.

- *Low costs of the recreational and commercial RPASs.* Any recreational or commercial RPAS, with features that could be exploited for malicious acts, are available starting from less than one thousand Euro without restrictions. Comparing prices between any commercial RPAS and a C-RPAS, the forces which are using malicious RPASs are far and away in advantage. So far there are no C-RPAS with one hundred successful rates. For terrorist forces, it is worth spending money on even dozens of RPASs if only one finally gets the target.
- *Weakness of the export control*. Recreational and commercial RPASs which are subject of this paper are not under export-import regulation control as dual use goods neither of US or UE legislation.
- *Gaps into existing regulatory framework*. There are two distinguish issues that must be taken into account. First one is regarding changes needed on control, registration, trading and using of recreational and commercial RPASs. The second one goes on further and highlight that it should carefully rethink legal challenges on using C-RPAS tools. We have to respond to some challenges like how it is perceived the privacy violation or how can we legally label and treat as hostile or at least malicious the RPASs which cross a perimeter. There are legal references which convict destruction or taking away someone else's proprietary without the permission of the owner, jamming or interfering with authorized radio communication, damaging an authorized computer program, and so on. A C-RPAS operator could be charged with kinetic effects of the RPAS depending on the outcome if he has done a physical attack. If the challenges of legal deployment of these systems are not taking into account, the investments will be put at risk and more than this it will even boost the impact level of the malicious RPASs operation. Following these challenges, some C-RPASs providers state on their websites the restrictions on their using[21].
- *Lack of the effective C-RPAS technology*. At the moment of writing this paper there have been a lot of the C-RPASs available both for military and commercially uses. A comprehensive market survey was released by Sandia National Laboratories [3]. It is important to spot out that in this moment there is not a common standard for an effective C-RPAS technology which could guide potential developers of these systems. On the other hand, a common counter RPAS technology is nearly impossible to design if we take into account the technical and deployment challenges, regulatory frameworks and so on.

[20] BI Intelligence, 2016, June 10, "THE DRONES REPORT: Market Forecasts, Regulatory Barriers, Top Vendors, and Leading Commercial Applications," Business Insider, accessed June 2, 2017, http://www.businessinsider.com/uav-or-commercial-drone-market-forecast-2015-2

[21] "Counter-UAS Technologies," accessed February 19, 2017, https://www.battelle.org/government-offerings/national-security/tactical systemsvehicles/tactical-equipment/counter-UAS-technologies

- *Deployment challenges.* It is hard to develop a C-RPAS system that can meet challenges of the all environments were a malicious RPAS could be used as threat or weapon. A malicious RPAS could be used against any critical infrastructure, residential areas, over maritime and land border, crowded places and urban environmental, during some major events and so on. Also, it could be used during day or night time and different meteorological conditions. In other words, it would be used nearly against any civilian target in any environment. Even though an effective low-cost C-RPAS could be made available, the financial, personal and maintenance deployment cost at all national possible target exceed the nation's capability.
- *Misunderstanding by the different decision levels of the real threat dimension*. Decisions regarding all important regulatory countermeasures addressed to the potential RPASs used in malicious acts are taking at different administrative and political levels. Understanding at all these levels of the real dimensions of the threats and the impacts on citizen privacy and safety or on national security as a result of the critical infrastructures attacks, it is the key for the success of a strategic implementation of a C-RPAS plan.
- *Technological rapidly development*. Recreational and commercial RPAS cannot be kept away from nowadays technological development that bring up new RPASs features or capabilities of flying, command and control or resistance against countermeasures. For example, an extreme impact on countermeasures domain was the evolution from recreational and commercial RPASs flying without GPS (first person view) to GPS location awareness and flight controller. RPASs could be used in more and more difficult environments and artificial intelligence allow them to operate in swarm collaborative mode[22].
- *Most of the recreational and commercial RPASs are already getting ISTAR capabilities*. So far, the ISTAR capabilities have only been at disposal of military RPASs. All ISTAR capabilities (information, surveillance, target acquisition and reconnaissance) are nowadays common for all commercial RPASs and even for some of the recreational RPASs.
- *Recreational and commercial RPASs could be easily modified to get military features and capabilities.* There are reports that highlight that ISIS is investigating modifications to commercial RPAS through really well-organized programs in order to mitigate possible RPASs counter measures and increase their lethality and effectiveness of operational characteristics [1].
- *Environments were malicious RPASs can be used*. The environments were malicious RPASs can be used is a more and more busier radio frequency spectrum, a noisier background and more and more flying objects are seen. All these imply a more complicated and costly technical solution for an effective counter RPAS because it is more and more difficult to detect and classify a malicious RPAS.

[22] http://www.swarmsys.com/

III. COUNTER RPAS

Military forces or law enforcement authorities need a C-RPAS with not only theoretically but also practically nearly 100% demonstrated successful rate.

C-RPAS systems, in order to fulfil all their operational functionalities, must work according to a "kill chain" model. A Sandia National Labs report defined a three step "kill chain" model: detection, classification and neutralization [3]. We have added at this model other two phases: tracking and forensic. Therefore, the model has been becoming a five "kill chain" model: detection, classification, tracking, neutralization and forensic. An effective C-RPAS system must successfully carry out each step strictly in this chain order.

There are multiple types of RPASs with different range of action. It is obvious that must be a correlation requirement between detection range and neutralization range on one side and the RPAS operation range on the other side.

An effective C-RPAS need to be versatile and set off its strategies accordingly to the type of attacks (e.g., singular or swarm attacks). Moreover, the C-RPAS must integrate automatized effectively all phases from detection, classification, tracking and lock-on to a target up to a successful neutralization (Fig. 1).

Detection

In this phase, a large number of heterogeneous sensors organized into a sensors network are collecting information from a cluttered noisy background environment data. The sensors must be deployed in accordance with their effective range, with the aim to defeat the whole zone protected (named also the responsibility zone of the counter RPAS). The responsibility zone is defined in 3D dimensions with a half-sphere shape.

In order to be effective, the sensors used in detection phase must complement with neutralization and tracking phases.

It is necessary to use a complete mix of sensors because:

- There are a large variety of RPASs which must be detected, with very different characteristics (e.g., cross section, speed, acoustic and radio signature, flying mode). Consequently, there is not a single sensor type appropriate to any possible malicious flying object. Sandia National Laboratories has done an evaluation of effectiveness of different sensor types according to three types of RPAS – glider, quadcopter and jet turbine [3]. We have completed the list with a new state–of–the-art one which is a passive radar that is using "electro smog" [8]. For evaluation was used a scale with three levels: good, mild and poor (Table II).
- There is a cluttered video, audio and spectral radiofrequencies background and consequently a mix between a lot of sensors boost the successful rate and lower the false positive and false negative rates. "The challenge for LSS threat detection for current high frequency sensors is the false alarm plots and how to engage with the real LSS threats that are in the velocity domain of clutter or natural objects such as birds, 'angels' or ground vehicles." [4]
- The attackers could use some measures with intent to impede the successfully detection of the malicious RPAS like using of the cellular communication or non-

standard frequencies for C2 link, fully autonomous mode and so on.

- In order to be full effective and to mitigate the threat at a high level, the C-RPAS solution must be addressed to both the RPAs and their Remote Controller Units (RCUs).

The most challenging issue for detection phase is that the amount of data required to provide a reasonable response time is very large.

Each sensor should assign a unique ID event and timestamp and then provide valuable information for classification and risk assessment (e.g., azimuth, elevation, distance, speed, propulsion, trajectory and so on) (Fig. 2).

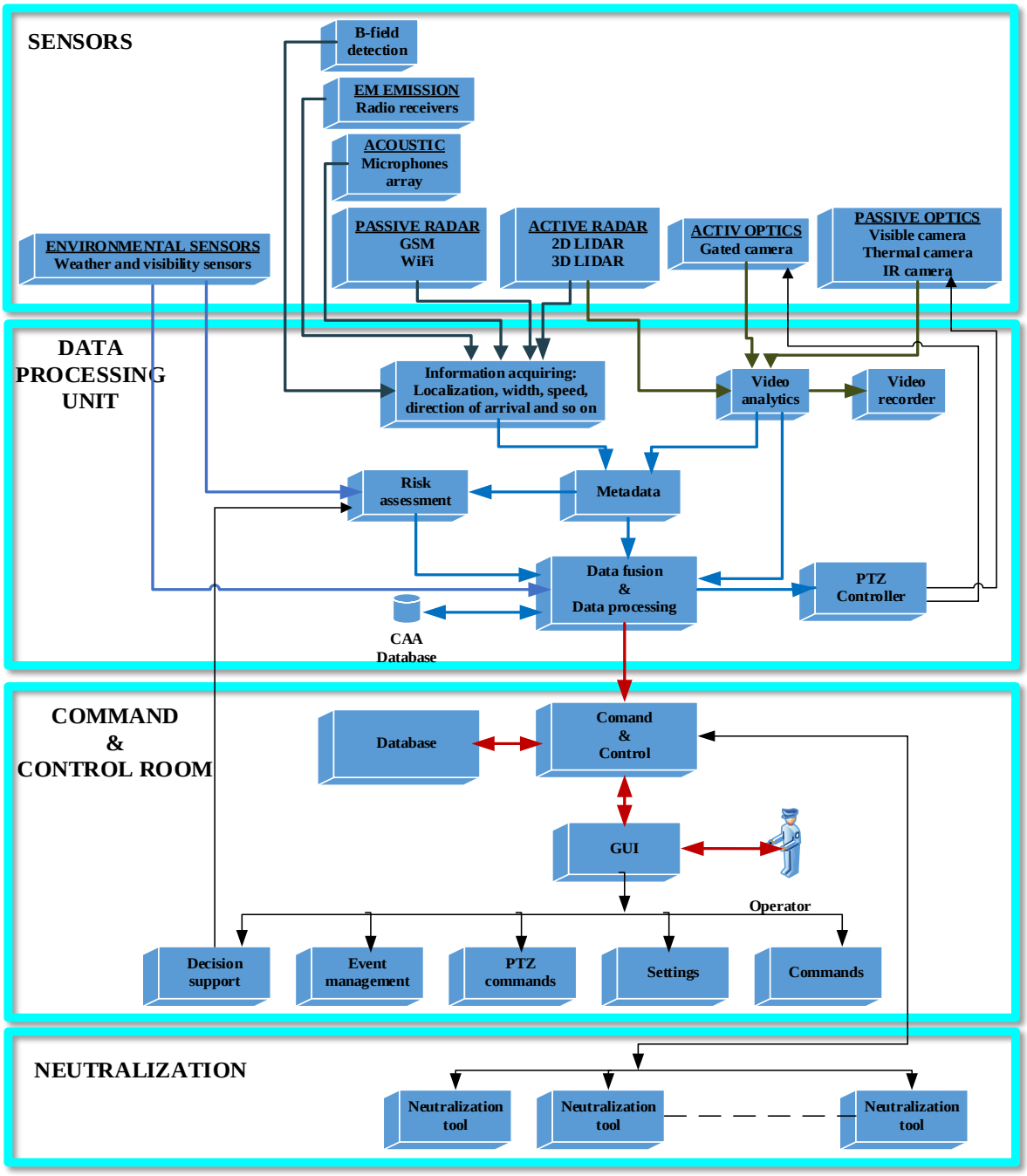

Figure 1. C-RPAS architecture

Classification

Data that has been collected by all sensors in detection phase is combined and processed by a specialized algorithm (into "Data fusion & Data processing" unit from Fig. 1) following strictly one by one three steps in order to decide:

- If the object detected is or not a RPAS;
- If the object detected and identified as a RPAS represents or not a threat;
- The target's level priority.

The environmental background scanned by sensors in detection phase is a cluttered and noisy one where there are a mix of multiple objects which could be easily confused with a RPAS. Therefore, the first task of the C-RPAS, in classification phase, must be to decide if an object into the responsibility zone of the C-RPAS is or not a RPA. Failure to correctly classify an object in this step may result in a false positive or false negative classification with an according implying in the following steps of this phase and

in the following phases – tracking and neutralization.

Not all RPAs crossing a perimeter should be automatically treated as hostile or malicious. Moreover, a C-RPAS system may be installed not only in "no fly zones". Once an object has been identified as RPA, it must be evaluated and classified further as a threat or not. This process could be done through a preliminary assessment and decision that RPAS is or not an authorized one. This decision is taken after interrogation the Civil Aviation Authority (CAA) database. The object validation as a threat must be done firstly by machine, confirmed by a human operator, labeled accordingly and displayed into a GUI.

TABLE II. EFFECTIVENESS OF CURRENT SENSORS USED AS DETECTION OPTIONS

Sensor	Remarks	Flying objects		
		Glider	Quadcopter	Jet
Active radar	The radar cross section (RCS) for two small commercially available platforms was measured to be -15dBm2 and is theorized to be -30dBm2 if the RPA is constructed with an RF transparent material [4].	Poor	Mild	Between poor and mild
Passive radar [8]	It uses existing "electro smog" generated by GSM or WiFi systems as a source of illumination. It could be effective for large surfaces [8].	Mild	Mild	Mild
Passive optics (video, thermal or infrared cameras)	Imaging commercially available quadcopters with EO/IR visible, MWIR, and LWIR resulted in low contrast images, and the amount of data required to provide a reasonable response time is very large [4].	Mild	Mild	Between poor and mild
Active optics (LIDAR)		Mild	Mild	Poor
Acoustics	Acoustic detectors were successfully demonstrated and identified a UAS from 25 meters at an elevation of 10 meters using a microphone array [4]. Last projects relieve that acoustic sensors through an effective acoustical sensor network could detect commercial drones (DJI Phantom Drone) up to 300m [7].	Poor	Mild	Mild
EM emissions	RF detection is promising since currently available COTS RPAS technology requires a transmission and receive signal from a human user [13]. On the other hand, the detection of RF becomes highly complicated if a RPAS uses open source software or is programmed to require no human interaction.	Mild	Mild	Between poor and mild
B-field detection	Disturbances within the magnetic field around a RPA has potential to be detected, but it is dependent on the materials used and the physical size of the system.	Poor	Poor	Poor

RPAS risk level assessment

If the object was classified as a threat, it needs further to be assessed for a risk level in order to take the most appropriate response at a multi option neutralization phase. Sometimes the safety risk level of the effects of the counter measures could be higher than the potential risks of the offending RPAS. Moreover, there are scenarios when in responsibility area of a C-RPAS could be detected and confirmed as threats multiple heterogeneous RPASs with different parameters. Therefore, it is necessary to carry out a risk assessment process and finally to determine the risk level of the target. The level of the risk should be automatically calculated by an application based on certain parameters and then write down on target's label on the GUI of human operators. Risk level could be calculated according to the following parameters (Fig. 2):

- Type of target – "T". There are different types of RPASs as targets for a C-RAPS platform like glider, quadcopter, jet and so on. Each type has specifically characteristics which could make difference between them as level of risk – speed, altitude of flying, manoeuvrability, payload and so on.
- Direction of Arrival – "DoA". The targets could be headed to different points of interest or areas that are protected. Based on the risk assessment whole protected area could be sliced into sectors with different levels of importance.
- Range – "R". Represent the distance from the target to the point of interest or to the protected area.
- Velocity – "V". It is known also as speed.
- Estimated Time of Arrival - "EToA". It's computed based on velocity and range parameters (ratio between range and velocity).
- Number of the targets that have been detected and are tracking in the same time - "NoT". If the number of targets that are detected, tracked and showed on the GUI are increasing, the operator's activities are also increasing and in the same time these activities are more and more critic and difficult. On the other hand, it could be a scenario where multiple RPASs are working in swarm mode into an intelligent network. This last scenario is the most challenging for any C-RPAS.
- Number of the sensors that have confirmed the target - "NoS". Once a sensor gets information about a probable target this information is processed and sent to the specialized algorithm for preliminary detection and confirmation. Once more sensors send information about the same target, this information are getting into a fusion process growing the truthiness and trustiness level of the information about that target.
- Altitude – "A". The targets which are flying lower are considered more dangerous than targets which are flying at higher altitude.
- Interrogation results of other data bases – "DB". The C-RPAS system should be interconnected to the CAA database into which the RPAS have been registered and authorized for flying over the protected area. If the RPAS detected is not confirmed by the CAA

database, then it must be flagged and warned the human operators.

- Target's size – "W". As the target's size estimated by the video sensors is larger and larger, the target's threat level is increased accordingly. It is well known that a larger RPA can carry heavier dangerous payloads.

Tracking

Once information about a potential target has been acquired by one or multiple sensors this information is sent to a specialized module for intelligent fusion and processing, target validation and alarm generation

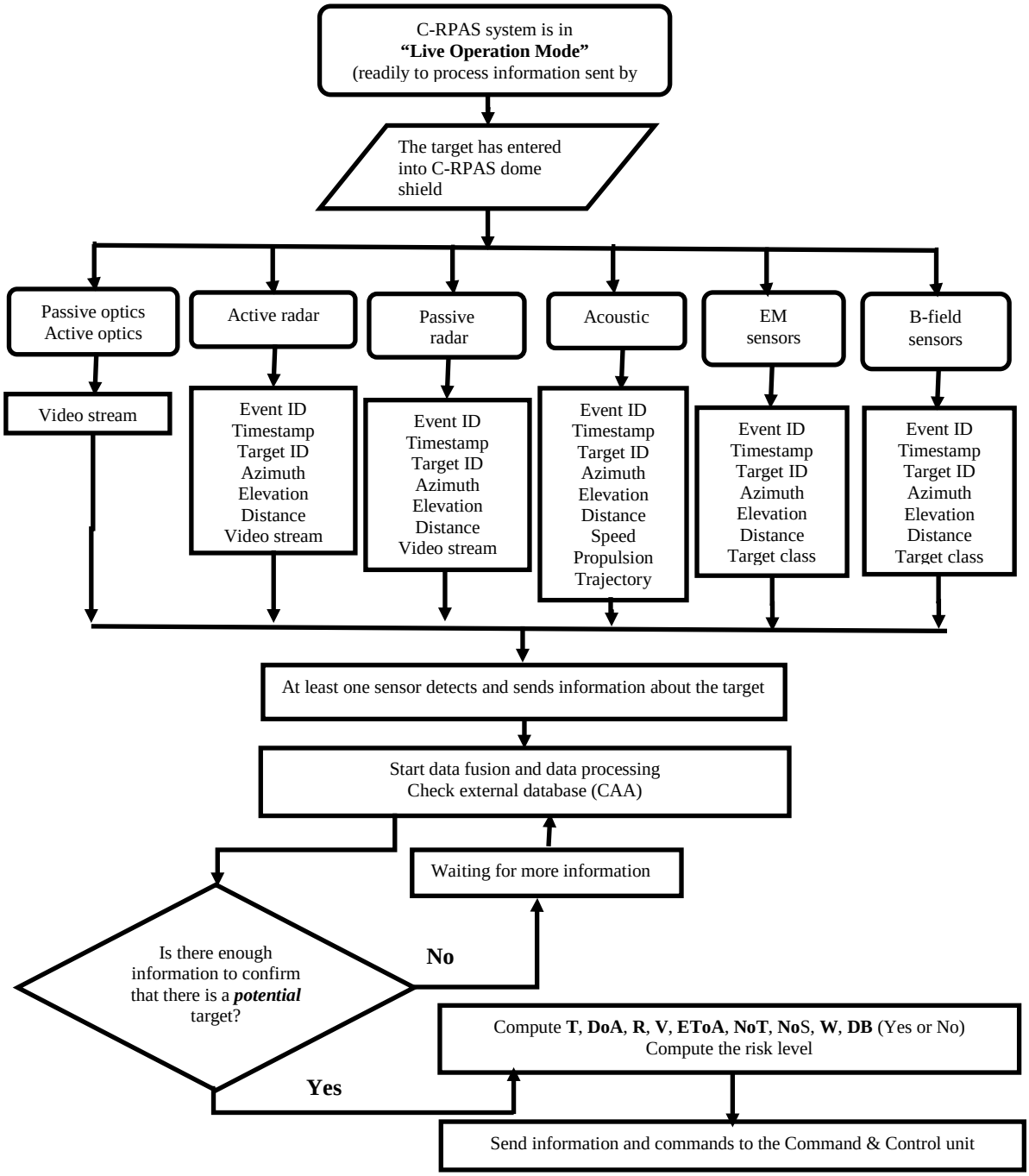

Figure 2. Detection, classification and risk level assessment

At the fusion level, "handover" procedures will be implemented to properly track the targets crossing more than one sensor set (thus, the alarm will be then displayed on the GIS map with its tracking path and target ID). Information about the target type and its level of threat will be also given, by applying methodologies from previously classification phase.

In order to get more time for the follows phase an initial coarse tracking will be put in place. A continuous process based on anomaly detection theory, statistical signal processing coupled with well-defined rules for intruder behavior analysis will be used. The goal is to discriminate, among the detected events, between normal or anomalous behaviors (forbidden trajectories, violation of flight regulations, suspect patterns). Finally, once a threshold for information necessary have been acquired and processed, a fine tracking will be implemented.

Handover procedures must take place automatically, and information about the active system(s) will be reported on the GUI. The full track is recorded for post-incident analysis.

Neutralization

The goals of the neutralization phase are:

- Deny RPAS's mission (mostly non-destructive) or,
- RPAS's neutralization (mostly destructive).

Based on the results of classification phase and specially on results of risk assessment, an intelligent C-RPAS should dynamically chose to carry out the appropriate method to meet one of the above goals.

The neutralization method needs to be chosen according to the environment (e.g., urban, isolated, operational requirements, battlefield) and to the effect of the method (e.g., destructive or non-destructive).

There are a lot of neutralization solutions each of them with its own weakness and strength points depending on technical implementation, goals and its applicability [3].

Geofencing

Geofencing neutralization consists mainly in design a virtual perimeter which becomes a restricted area based on "no-fly zones" configuration.

Strengths:

- This solution is 100% effective for prevention an unintentional flight to enter in a restricted area.
- It is a passive solution and consequently there are not contradictions to legislations regarding property, hacking, interference, damaging an authorized computer program, and so on.

Weakness:

- It is completely ineffective against intentional intrusions.
- There are hardware solutions through which "no-fly zones" configuration could be defeated.
- GPS system could be easily removed and an operator could directly conduct the RPA.
- Lack of the useful forensic evidence.
- "No-fly zones" configuration is available for DJI products only.

Potential solutions to strength the geofencing solution:

- By legislation all RPAS must be available with "no-fly zones" configuration.
- Military-grade encryption in order to prevent a terrorist from tampering with critical configuration like "no-fly zones", altitude, flying without GPS control, so on.

Physical or kinetic solution

In this category are included solutions like firearms, laser system [7],[9], missiles, gun nets, RPASs and birds.

Strengths:

- This solution is the simplest and the cheapest.
- There are few positive experiences regarding deployment of some solutions in USA.
- It is time effectiveness.

Weakness:

- It requires a high skill for operator.
- It has a very limited range.
- It is ineffective against RPAs which are moving at very high speed and with unpredictable changing of direction.
- It could be an adverse dangerous effect in use case of RPA target which is carrying explosive or dangerous materials.
- Birds' training is difficult, at very small scale available and birds could be injured which is in contradiction with legislation regarding bird's protection.
- It is in conflict to legislations regarding property.
- When firearms are using, forensic evidences are destroyed.
- There are aiming the RPAs but not the remote controller too.

Potential solutions to strength the physical or kinetic solution:

- It is necessary to work on regulatory framework to eliminate any legality issue which could arise regarding property rights.
- In order to be effective, must be done automated by machine following information from previous phases.
- It must be used only after an effective risk assessment regarding the consequences of its using.

Jamming

This neutralization solution has been tested and demonstrated in military domain as an effective one against various threats which are using radio frequencies [3],[4]. As a C-RPAS solution, it is aiming GPS signal navigation and command and control radio frequencies used for flight control, telemetry and manual operation.

There is a very large scale of jamming applications from pointing jamming up to High Power Electromagnetic Weapon (HPEW). HPEW transmits electromagnetic signal somewhere between 10 kHz up to several GHz and at power levels of gigawatts. The effect is ranging from temporary disruption to physical destruction of unprotected electronics.

Strengths:

- It is the most effective for nearly all commercial RPASs when GPS and command and control signal are both jammed.
- There are solutions on place which are getting good reports regarding their effectiveness[23].
- These solutions are relatively inexpensive, easy to operate and suitable in the most scenarios.
- These solutions increase the cost and technical complexity for an attack. On this purpose, the terrorists have already taken into account some counter measures against them[24].
- There are aiming both RPA and remote command and control unit.
- It is time effectiveness.

Weakness:

- If the GPS signal is jammed only, the RPAS operator could switch on manual operation and fly without GPS signal.

[23] "Counter-UAS Technologies," Battelle, accessed February 13, 2017, https://www.battelle.org/government-offerings/national-security/tactical-systemsvehicles/tactical-equipment/counter-UAS-technologies.

[24] Eric Schmitt, "Papers Offer a Peek at ISIS' Drones, Lethal and Largely Off-the-Shelf," The New York Times, January 31, 2017, https://www.nytimes.com/2017/01/31/world/middleeast/isisdrone-documents.html

- Most of the commercial RPASs are designed with "return to home" (RTH) or hover mode when they have lost command and control signal.
- It is ineffective against RPASs which are configured to operate in fully autonomous mode, or visual guidance systems. A malicious operator could disable the "return to home" feature in order to continue flying in autonomous mode in the event of control link loss.
- It is hard to jam C2 link when are used cellular communications on command and control purpose.
- The effects could be adverse when it is used against RPA carrying explosive or dangerous materials.
- In most countries, it is in contradiction to legislation regarding interferences which would stop using legitimate radio terminals, public or even emergencies services.

Potential solutions to strength the jamming solution:

- It is necessary to work on regulatory framework to eliminate any legality issue which could arise regarding interferences.
- It is necessary to find solutions to grow up the detection phase effectiveness in order to show exactly what frequencies are used for command, control and telemetry.

Hacking

Whereas in the jamming solutions it is necessary to know the frequencies used only, in the hacking solutions it is necessary to know both the frequencies and the protocols used. The objective of the hacking is to take the RPAS's control by breaking C2 link or insert malware on onboard flight controller. Most off the shelf commercial RPASs are equipped with poorly secured communication link used to control RPASs' flight directly or through a remote controller. A C-RPAS based on hacking technique could scans the frequencies, detects the frequencies in use and then sends the signals in order to take over the RPAS's control from the malicious operator and forces finally the RPAS to land or terminate its flight[25] [1],[8]. The hacking solutions are trying to exploit the terrorists' difficulty to replace the C2 link and lacking of cryptographic mechanisms.

Strengths:

- The aim of this solution is to land safely the malicious RPAS and reduce the collateral damage.
- There is a good conservation of the evidence for future forensic.

Weakness:

- Some of the RPASs could be controlled through non-standard radio links. In these cases, it is harder to hack on control link even if it is still possible to scan and detect the used frequencies.
- Some of the RPASs may be controlled through public cellular networks[26] [14]. In these cases, it is nearly impossible to detect and hack command and control link due to the capability of the cellular networks to work in extremely challenging environments.
- Even if it is difficult, malicious operators could disable link control of the commercial RPASs and then operate them in a fully autonomous mode.
- This solution is relatively expensive and complex to operate.
- Time is critically in lack of an automated hacking method.

Potential solutions to strength the hacking solution:

- It is necessary to work on regulatory framework to eliminate any legality issue which could arise regarding property and damaging an authorized computer program.

Neutralization summary

It is obvious that the neutralization solution largely depends both on risk assessment and on the RPAS's technical capabilities regarding navigation, command and control. The correspondence between RPAS's capabilities and the appropriate neutralization solution is summarized in Table III.

At first view, we can claim that there is at least one neutralization solution whatever the RPAS capabilities. This statement is not quite satisfactory because the effectiveness of the solution is finally the matter of interest.

We have scaled the level of threat for each RPAS's capability apart and the estimated level of effectiveness for each neutralization solution correspondingly. There are few interesting observations:

- For each RPAS's capability there are more neutralization solutions with different level of effectiveness.
- Effectiveness depends largely on how accurate detection phase was and the time at disposal for neutralization.
- The evidences from forensic phase greatly depend on results of the neutralization phase (i.e., its destructive effects).
- It seems that more than one neutralization solution is necessary in the same time like in detection phase when all types of sensors are needed.

Forensic

The forensic is logically the last phase of a counter RPAS process which has to meet the following objectives:

- Establish who is the owner of the RPAS and for what purpose it was used for.
- Retrieve the flight path and the home point.
- Retrieve valuable information from application databases installed into remote controller and mobile device.

In the first step, it is recommended to obtain a forensic image of all system and memories files from all RPAS components. In order to conclude what file has been modified it is obviously that we must know the initial state of these files.

The forensic activity envisages the following RPAS components [10],[11]:

- RPA.
- Sensors.
- Remote controller.
- Mobile device.

[25] Samy Kamkar, "Samy Kamkar - SkyJack: Autonomous Drone Hacking," accessed February 13, 2017, http://samy.pl/skyjack/.

[26] http://www.g-uav.com/

TABLE III. MATRIX OF NEUTRALIZATION SOLUTIONS

RPAS's functionalities / capabilities					Probability Rate to occur	Neutralization solutions							
						Geofencing		Physical / kinetic		Jamming		Hacking	
GPS	Standard C2 link	Non-standard C2 link	Cellular C2 link	Fully autonomous		Applicability	Effective rate	Applicability	Effective rate	Applicability	Effective rate	Applicability	Effective rate
√	√				High	√	Low	√	Moderate	√	High	√	High
√		√			Low	√	Low	√	Moderate	√	Moderate	√	Moderate
√			√		Moderate	√	Low	√	Moderate	√*	Low		
	√				High			√	Moderate	√	High	√	High
		√			Low			√	Moderate	√	Moderate	√	Moderate
			√		Moderate			√	Moderate				
				√	High			√	Moderate				

** - most probably for GPS only*

First of all, it is necessary to evaluate physically all components of the RPAS and note the type of the each component, serial number, payload, sensors, or any evidence which could point out for what purpose have the RPAS been used on.

The main elements of the RPA which need to be investigated are GPS and Flight Controller.

Through GPS are received geographic coordinates from satellites which then are transmitted to the Flight Controller and camera. Without GPS, RPA is unable to take-off. Nevertheless, it is possible to block GPS by attaching an opaque electromagnetic tin foil over the GPS receiver. In this case RPA is no longer acquiring home position and RPA could fly over restricted areas.

The most important information and artefacts which could be retrieved from Flight Controller are related to OS, Flight Controller ID, flight data records (e.g., home position, flight path), data about RPA components (e.g., motor load, motor speed, battery load, battery voltage, system failure), information about boot sequence, maintenance and logistic.

The types of sensors which have been found attached to RPA tell us about the purposes of the flight (e.g., optical, thermal, LIDAR, NIR, WiFi). From sensors could be exported images files, video files and EXIF data. EXIF data point out information about the camera and where the pictures were taken through geographic coordinates and altitude therefore rebuilding a 3D scene. The EXIF data are persistent even after the RPA has crashed. The relative time between media recorded remain the same even if the system time was tampered.

From Remote Controller application memory, we could retrieve some artefacts like:

- Vendor applications, owner name and account.
- Default settings.
- Launch points, dates. Launch point recorded for every start up so you can plot onto the map where RPA was previously launched.
- Association of geographical coordinates to GPS data from media.
- Mission plan and flight telemetry data.
- Connection logs to cloud services and user credentials for log to cloud.

Usually between the Remote Controller and human operator there is a mobile device or tablet. Into mobile device there are a lot of valuable information:

- About OS. It is worthwhile to highlight that the time on all components and applications of the RPAS is synchronized with the mobile OS.
- Application for settings and control the flight.
- Subset of data recorded on the Flight Controller.
- Imagines, video and Flight Controller ID.

A counter forensics should not be neglected in order to determine if the integrity of evidence has been modified or the time stamp was tampered.

If the RPA is powered up when the investigation starts, it must dump the memory before any action is taking. In situation of cold forensic, the only information that could be retrieved from RPA is recorded media and related EXIF data.

There are web sites were files retrieved from RPAS components could be sent for online parser[27].

IV. SAFESHORE PROJECT FOR DETECTION CLASSIFICATION AND TRACKING OF MALICIOUS RPASS

The European Commission noted that there is currently a discrepancy between on one hand strict rules for access to airspace and on the other hand a poor capability to detect illegal operations. Therefore, the European Commission decided to fund the SafeShore project, which focuses on the detection of threat agents like RPAS in a marine border surveillance scenario.

The main objective of the SafeShore project is to cover existing gaps in coastal border surveillance, increasing internal security by preventing cross-border crime such trafficking in human beings and the smuggling of drugs. It is designed to be integrated with existing systems and create a continuous detection line along the border. One of the treats to the maritime coast are small Remotely Piloted Aircraft Systems which can carry explosives or which can be used for smuggling drugs, boats and human intruders on the sea shore. The mini-RPAS can depart from maritime platforms such as yachts. Their low cost and very small signature makes them a favorite platform for smugglers and terrorists. The mini-RPAS Radar Cross Section is too small to be detected by the regular costal radars, which is where SafeShore comes in.

[27] https://airdata.com/

The SafeShore core solution for detecting small targets that are flying in low attitude is to use a 3D LIDAR that scans the sky and creates above the protected area a virtual dome shield. In order to improve the detection, SafeShore will integrate the 3D LIDAR with passive acoustic sensors, passive radio detection and video analytics. The boats and humans on shore will be detected by a 2D LIDAR integrated with video analytics. Those technologies can be considered as low cost and "green" technologies. It is expected that a combination of orthogonal technologies such as LIDAR, passive radio and acoustic and video analytics will become mandatory for future border control systems in environmentally sensitive areas.

The SafeShore objective will be to demonstrate the detection capabilities in the missing detection gaps of other existing systems such as costal radars, thereby demonstrating the capability to detect mini-RPAS along the shore and the sea or departing from civilian boats.

Another important SafeShore goal will be to ensure fusion of information and increasing the situational awareness and better implementation of the European Maritime Security Strategy based on the information exchange frameworks – EUROSUR and EUCISE 2020 while ensuring the privacy of the data and conformity to internationally recognized ethical issues concerning the safety of the information and the equipment subject of the project.

V. Conclusion and Future Work

It is obvious that using commercial RPASs by non-state actors on malicious purpose cannot be avoided through current technical and regulatory solutions.

Prior to sketching a C-RPAS solution it is necessary to update the international and national legislation regarding the status of these RPASs and the conditions of use within non-segregate space. The RPASs are aircrafts and must therefore fully comply with the rules on aeronautical safety, air traffic management, pilot licensing and aeronautical certification of the aircrafts.

In parallel with legislative initiatives, efforts should be continued to achieve an effective C-RPAS solution with an acceptable percentage of false positives and false negative errors. This solution needs to meet few key requirements:

- Must be completed therefore it would have to include detection, classification, risk assessment, tracking and neutralization.
- Detection phase must include all state of the art sensors (e.g., optical, radars, acoustic, electromagnetic and so on).
- Neutralization phase must include alternative solutions and the choice of one of them must be done in accordance with fusion and processing data, risk assessment and validated by human.
- The last phase must be the forensic when the artefacts are analyzed. The information gathered is essential for future preventive and reactive measures.
- Entire C-RPAS solution must be designed and implemented through standard interfaces. This requirement is essential for future interconnection with other complementary solutions and LEA's command and control rooms.

All these desires cannot be achieved if there is a lack of a strong RPAS community which gather people of the main fields: LEA, research and industry. We have worked on this paper taking into account the need to strengthen the existing RPAS community and offering valuable information for them[28].

There are a lot of research topics that can be done on the RPAS field, now and as technology, tactics, and laws evolve. Some possible future efforts include:

- Demonstrative forensic on the most used commercial RPASs.
- Create a specialized RPA forensic community and forensic database which would be accessed by all authorized persons.
- Investigate the impact of using 4G/LTE technology inside commercial RPASs for video channel and command and control.
- Examine proposed regulatory changes to determine possible impact.

Also, we are working on preparation the testing phase of the prototype of the SafeShore project. Practical tests will be carry out in real environmental conditions at three different locations: North Sea, Mediterranean Sea and Black Sea.

References

[1] D. Kovar, "Defending Against UAVs Operated by Non-State Actors," The Fletcher School, Tufts University, Final Thesis, GMAP 16, https://integriography.wordpress.com/2017/03/24/defending-against-uavs-operated-by-non-state-actors/

[2] Commission Regulation (EC) No. 262/2015 of 7 December 2015 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and repealing Regulation (EC) No 216/2008 of the European Parliament and of the Council.

[3] Gabriel Birch, John Griffin, and Matthew Erdman, "UAS Detection, Classification, and Neutralization: Market Survey 2015," Sandia National Laboratories, 2015, http://prod.sandia.gov/techlib/access-control.cgi/2015/156365.pdf.

[4] The NATO Industrial Advisory Group Study SG-170, "The Engagement of Low, Slow and Small Aerial targets by GBAD," July, 2013.

[5] Qiao Liang and W. Xiangsui, "Unrestricted Warfare," Nov. 10, 2015

[6] http://safeshore.eu/

[7] M. Laurenzis, et al., "Detection of small UAVS – Project OASyS2," Security Research Conference 11th Future Research, Berlin, Sep. 13-14, 2016.

[8] W. Koch, "On multiple sensor UAS security. Research aspects and first experimental results," Security Research Conference 11th Future Research, Berlin, Sep. 13-14, 2016.

[9] K. Ludewigt, Th. Baumgartel, Th. Riesbeck, J. Schmitz, A. Graf, and M. Jung, "High Energy Laser Weapon demonstrators for C-UAS applications," Security Research Conference 11th Future Research, Berlin, Sep. 13-14, 2016.

[10] M. Maarse and L. Sangers, "Digital forensics on a DJI Phantom 2 Vision+ UAV," University of Amsterdam, Apr. 29, 2016.

[11] D. Kovar, G. Dominguez, and C. Murphy, "UAV (aka drone) Forensics," SANS DFIR Summit Jun. 23-24, 2016.

[12] International Civil Aviation Organization, Unmanned Aircraft Systems (UAS), 2011.

[13] "ARDRONIS evolves UAV detection," *Jane's Airport Review*, Jun. 2017, Vol. 29, No. 5.

[14] Leading the world to 5G: Evolving cellular technologies for safer drone operation, https://www.qualcomm.com/invention/technologies/lte/advanced-pro/cellular-drone-communication, accessed Jun. 24, 2017.

[28] www.uvsr.org