SMALL UNMANNED AERIAL VEHICLES – THREATS AND DEFENCE AGAINST THEM

Jakub VILÍMEK

Abstract: The article discusses actual small UAVs (Unmanned Aerial Vehicles) threats and ways of defence against them. The introduction contains UAVs regulations in the Czech Republic. The literature review of relevant papers in the UAV threats and defence follows. The third part is about off-the-shelf and professional UAVs, which can be misused to attack. The core of this article describes three vital processes for planning UAV protection: detection, identification and elimination. The goal of the article is to define vital questions, which has to be answered before designing any UAV protection system. The correct answers to these questions depend on the protected area, assets, etc.

Keywords: UAV; UAS; Threat; Detection; Protection; Sensors.

1 INTRODUCTION

Unmanned vehicles (land, aerial, surface and underwater) are very popular and actual topic today. The market is flooded with professional and amateur unmanned vehicles. On this fact reacted most of the nations' authorities and created some legal restrictions on UAV[1] usage.

The legal framework of UAVs usage in the Czech Republic is defined in the Regulation L2, Rules of the Air, Attachment X [1]. Attachment X restricts usage of UAVs in certain areas for all the time (e.g. airfield protection zones, restricted areas around nuclear plants, army objects, dangerous areas – gas release areas, etc.), or for certain time of the day (e.g. military training areas during the training).

Attachment X also restricts the minimal distance between UAV and persons, buildings and inhabited areas. The distance for small UAVs (up to 7 kg) is the distance described as safe[2]. This distance for UAVs heavier than 7 kg is again recommended as safe but the Attachment X orders minimal distances as well: 50 m for starting and landing, during the flight UAV cannot be closer than 100 m to persons, assets or buildings, which are not related to the flight. UAV cannot be closer than 150 m to any densely populated area [2].

The violation of the legal framework can be done by negligence or on purpose. The presence of the UAV in the restricted area (e.g. airfield vicinity) can disturb security or safety of the whole area. An intentional presence in the restricted areas can have various reasons.

UAVs can simply collect imagery, or in general sensor information and with this imagery the UAV's operator can search for weak spots in the security of the area of interest (airfield, ammunition dump, nuclear powerplant, etc.). In this case the UAV is just a first step before frontal assault on the protected object.

Next reason of the UAV's presence in the restricted area can be a direct attack with weapons or explosives attached to the UAV. Attachment X [1] forbids loading and transporting any dangerous substances or devices, as well as dropping any objects during the flight[3].

A price of an off-the-shelf UAV with improvised explosives is very low in comparison with possible effect, inflicted damage and injuries. Very unlikely scenario describes possible attack with a radioactive or poisonous material, explosives, both attached to the UAV. This UAV can fly over densely populated area, unprotected water source, etc. and then it can explode as a "dirty bomb".

Possible types of attack must be considered during planning any small UAV protection of the areas with critical infrastructure, or areas with high concentration of people. Next question is the type of UAV – amateur, professional or even military. Next level of any protection planning is protection against the whole swarm of cooperating UAVs. This type of attack exceeds scope of this article and it was not a part of the literature review.

2 THE LITERATURE REVIEW

The literature review was oriented to Scopus indexed papers with the goal to find the relevant papers in the theme "(UAV or UAS) and threats and (defence or defense)". The topic was found in 105 articles (on April 30, 2019), the result of the search was sorted by "Newest" and for further inspection were chosen only the most relevant 8 articles; see [3] to [10].

New problems with the fight against UAS were caused by the technology in the development of commercial drones that are available to the

[1] In the article will be used following terms: UAV: Unmanned Aerial Vehicle (drone), UAS: Unmanned Aerial System (UAV, control station, devices for communication, start and land). Sometimes the term UAX (UAV or UAS) is more suitable.

[2] The Civil Aviation Authority in the Czech Republic recommends the save distance as ration of 1:2 during forward flight (each 100 altitude meters safe radius 200 meters) and 1:1 during hovering (each 100 altitude meters safe radius is 100 meters) [2].

[3] Articles 10 and 11.

population without any problems. They can also be used in war and crisis situations; they can act as "paparazzi" and can be misused by criminal and terrorist entities. The primary task is detection in a fight against UAVs.

The paper [3] summarizes series of very complex measurements, that were performed by the authors during past 4 years. The experiments involved small UAV detection by radar (RL), radio frequency (RF), electro-optical (EO), infrared (IR), acoustic (AC); and detection by human senses (eyes and ears). The authors strongly suggest, based on the measurements results, using multispectral detection, building modular defence systems. The real-time detections are possible at these distances:

- standard X-Band radar: 3000 m;
- optical devices with zoom and skilled operators: 2000 m;
- infrared detectors: 350 m;
- personal audibility (unarmed ears): 250 m;
- personal visibility (unarmed eyes): 350 m.

UAVs are used in wide range of human activities and the amount of UAV users are growing rapidly. The risk of misuse of UAVs by criminals, guerrillas or terrorists is the actual threat. Importance of developing scientific fields for countering of UAVs rises. Areas of threats and defence include parts: Air surveillance; Command and Control; and Elimination [4].

UAV is becoming a threat to sensitive areas' defence, public safety, and privacy. For the difficulty of supervision, prevention, evidence collection, and punishment, the UAVs management is an urgent problem. The control signal of UAVs is an object for research with a goal to find the interference signal for smart jamming. Signal analysis using MATLAB was realized in time and frequency domain. Study of the typical civilian small UAV's communication protocols, and using the software defined radio to receive and store the control signals. After demodulation and data decryption are the signal parameters estimated effectively; the parsing command signal was used for generating the inference signal [5].

According to the study [6] the air defence used for civilian purposes, can include the long-term threat assessment and anticipation, infrastructure assessment, surveillance, tracking and imminent threat assessment, UAS target engagement and operator detection and capturing, and initiation of actions against UASs to prevent the intentions of rogue drones.

Nowadays, unconventional Low Slow and Small (LSS) air threats pose serious challenges that cause deep concerns among military and civilian security organizations. Consequently, there is a high demand for robust and reliable counter small unmanned aerial vehicles (C-sUAV) solutions. Detection challenges such as small air targets, unconventional flight patterns in low airspaces, terrain masking effects, or complex urban environments lead to high false alarm rates. Current C-sUAV systems in the market use improved radar components, originally either considered for VSHORAD[4] radar, battlefield radar, bird detection radar, perimeter surveillance radar, or high-resolution short-range radar [7].

The NATO has defined UAV categories in class 1 [7], see Table 1.

Table 1 NATO UAV class I

Type of UAV	Range	Altitude	Weight	Payload
Micro	5 km	100 m	< 2 kg	< 0.5 kg
Mini	25 km	1000 m	2 – 20 kg	< 10 kg
Small	100 km	1500 m	< 150 kg	< 50 kg

Source: [7].

An overview of the different sensors and properties can be found in Table 2.

Table 2 The sensor properties

	Long range	Position accuracy	Iden-tifica-tion	Multiple targets	Low visibility conditions	Night	Pas-sive
Visual	++	++	++++	++	-	-	++++
Infrared	++	++	++++	++	-[5]	++++	++++
Acoustic	-	-	+++	++	++++	++++	++++
ESM[6]	++++	++++	++	++++	++++	++++	++++
Human surveillance	+	+	++++	-	-	-	++++

Source: [7].

Research of the drone detection by means of different thermal imaging systems (infrared sensors) and development original thermal image enhancement algorithm for infrared scanner system is presented in the paper [8]. Main features of an infrared image, which are not occurring in case of visual images, are relatively low spatial resolution, low image contrast, presence of noise pattern or pulse disturbances.

The proliferation of LSS flying platforms brings with it a new and rapidly increasing threat for national defence and security agencies. Thus, defence systems must be designed to face such threats. Modern operational readiness bases on proper personnel training that is performed on high fidelity simulators. The aim of the paper [9] is to take into account the variety of the commercially available LSS aerial vehicles and to define LSS models from different points of view. The LSS can be modelled with respect to the behaviour during the flight and the user interface, signature against different type of detectors, and threat itself and the defence tactics.

While the technology for operating a single UAV is rather mature, additional efforts are still necessary

[4] Very Short Air Defence.
[5] Except SWIR (Short-wavelength infrared).
[6] Electronic support measures.

for using UAVs in fleets (or swarms). The Aid to SItuation Management based on MUltimodal, MUltiUAVs, MUltilevel acquisition Techniques (ASIMUT) project aims at investigating and demonstrating dedicated surveillance services based on fleets of UAVs. The goal is to enhance the situation awareness of an operator and to decrease his workload by providing support for the detection of threats based on multi-sensor multi-source data fusion. The operator is also supported by the combination of information delivered by the heterogeneous swarms of UAVs and by additional information extracted from intelligence databases. As a result, a distributed surveillance system increasing detection, high-level data fusion capabilities and UAV autonomy is proposed [10].

The summary of the literature review:

- New problems with the fight against UAS are caused by technology progress in the development of the commercial drones.
- UAVs are available to the population without any problems; UAVs can be used in war, crisis situations, and they can be misused by criminal and terrorist entities.
- Areas of threats and defence include air surveillance, command and control, and target elimination.

3 OVERVIEW OF OF-THE-SHELF AND PROFESSIONAL UAVS

The market is full of various UAVs categories. These machines can be equipped with various accessories based on their size, weight and battery capacity. Digital cameras are usually used for collecting information, but UAV can be geared with a lidar, a radar, a thermal camera or other sensors. UAVs can be also equipped with attached explosives or primitive drop mechanism, which release an explosive. UAVs can be also used for transporting a non-lethal cargo, mostly illegal (e.g. drugs, cigarettes and other contraband).

Size based classification of UAVs may differ in regions. The previously mentioned Attachment X [1] defines these categories based on their maximum take-off weight:

- ≤ 0,91 kg,
- 0,91–7 kg,
- 7–25 kg,
- > 25 kg.

The NATO uses slightly different classification, see Table 1.

Very similar UAVs classification is used in the paper called Multispectral Detection of Commercial Unmanned Aerial Vehicles:

Table 3 UAV Classes

Category	Range [km]	Altitude [m]	Operational time [hours]	Weigh t [kg]
Nano	< 1	< 100	< 1	< 0.025
Micro	< 10	< 250	1	< 5
Mini	< 10	< 300	< 2	< 25

Source: [3].

One other UAV classification:

Tab. 4 UAV type by usage

UAV Type	Price [€]	Video [px]	Flight Time [min]	Range [km]	Purpose
Amateur	< 200	1280x720	< 15	< 0.1	ISR[7]
Professional	> 800	4096x2160	< 30	< 8	ISR[7] + A[8]
Race/Custom	various[9]	4096x2160	< 30	< 4	ISR[7] + A[8]
Military[10]	> 4000	4096x2160	various[11]	various[12]	ISR[7] + A[8]

Source: [3].

3.1 UAVs for information collection

The author picked different size UAVs from the most known e-shop in the Czech Republic. The regulations don't require any failsafe system on these machines. This failsafe system would end the flight in the case that the communication between UAS and control station would be interrupted. Some of the representatives in this category can have a return command to the default position in their communication protocol. This command could be used in the taking over type of attack, because this command is usually standardized.

UAS created by the DJI company usually contains restricted areas, which are forbidden for UAVs to flight into. These forbidden zones are managed by the DJI company, which creates them based on data from the national authorities. The restricted zones can change during the time, so they are available online [12]. The company defines also a "Warning" zones, which can be entered after confirming that you really want to enter this zone. Next zone categories are Restricted and Authorization. Flight into these zones has to be permitted by the local authorities. In this case some type of UAV's registration has to be done.

[7] Intelligence, surveillance and reconnaissance – information collection.

[8] Attack – deliver explosive payload.

[9] Can start at 100 € and be up to thousands of €.

[10] These UAVs are usually out of the legal framework of Attachment X. It is a very wide group of UASs, which can be autonomous, which can cooperate in a swarm, etc. Planning of protection against this type of UAV is far beyond of this article purpose. So, they will not be further discussed.

[11] Larger UAVs can flight up to 24 hours. More advanced concepts with unlimited flight time are also in the development [11].

[12] These UASs are not limited thanks to a satellite communication between UAV and control station.

3.1.1 Syma X5SW PRO

Syma X5SW PRO [13] was in the model row SYMA X5C recommended [14] as the most suitable for the information collection. Like all X5C UAVs contains a 6-axis gyro for flight stabilization. It also contains HD camera with resolution 1280 x 720 px with ability to display a video stream on the smartphone. Flight time depends on the battery and it can be up to 20 minutes. Range is up to 100 m, which is very nice distance in the category of very cheap UAVs. According to the records available online, the video is not very good, but it still can be used for gathering some information. Control SW contains home return functionality.

3.1.2 DJI Mavic Air

DJI Mavic Air is very cheap representative of professional UAVs. But despite its low price it can offer a very good service to the potential attackers. Camera itself (not just the UAV's body) has a 3-axis stabilization and it supports a 4k video stream. With the weight of 430 g is still categorized as a Micro. Flight time is up to 21 minutes and with moving operator can flight up to 10 km on one charge. Maximum flight speed is up to 68 km/h. The UAV also contains a sensing system to avoid obstacles. This sensing system reduces maximum flight speed to 28 km/h. Control SW contains return home functionality. If the radio connection between UAV and control station is interrupted, the UAV will retrace its original flight route, until the connection is restored.

3.1.3 DJI Mavic 2 Enterprise (DUAL) Universal Edition

DJI Mavic 2 Enterprise (DUAL) Universal Edition [15] is the most equipped commercially available UAV[13]. The camera has a 3-axis stabilization and supports 4k videos as well. The UAV is also equipped with the Radiometric FLIR thermal sensor. The operator can have 3 types of imagery data – FLIR MSX, infrared spectrum or visible light spectrum. This provides whole new dimension of the information collection. The UAV can be equipped with the speaker, light or safe flight beacon. The discrete mode allows the operator to switch off the LED lights and make a hardly detectable night reconnaissance. An open terrain range is up to 8 km. The UAV was at first place designed for professionally usage – army, police, searching for persons in hardly accessible terrain, mass or natural disasters, energetics, telecommunications (mass inspections) [16]. But it is possible to buy it without any restrictions and potential attacker can gain very powerful tool for gathering information.

Table 5 UAVs for collecting information

UAV	Weight [g]	Size [mm]	Range [m]	Video Resolution	Price [€]
Syma X5UW PRO	967	320x70x320	100	1280x720	93
DJI Mavic Air	430	83x49x168	8000	4096x2160	860
DJI Mavic 2 Enterprise	910	322x224x114	8000	4096x2160	3000

Source: [3].

3.2 Direct attack UAVs

This article will not consider professional military UAS, as it was mentioned before. Due to the clear illegal intentions of usage are these UASs not commercially available. But it is not so hard to build an armed UAV by using two slightly different ways. Attacker can just attach a weapon or explosives to an off-the-shelf UAV; or the attacker can create a completely new UAS from obtainable components. This type of UAS was intentionally not mentioned before, but this does not mean, the attackers can't create a customized UAV platform, equip it with a stabilization mechanism, quality 4k camera and collect information with it.

3.2.1 Building custom UAV platform

How to build a custom UAV tutorials can be very easily found on the Internet, i.e. [17], [18]. These tutorials are very complex and skilled man is able to build this UAV. The custom UAV community is very open and a desperate builder can seek an advice there.

At first you have to choose a size of the UAV. Bigger size and thus payload are better for attack with explosives. It is possible to use online calculator [19] to verify, that designed UAV is flight-capable. This calculator also provides some expected flight characteristics based on many variables (number of rotors, type of motors, propellers size, battery capacity, etc.). With the help of tutorials, the designer is able to design the UAV core and then add weight and simulate size of the explosive payload. It is also possible not to attach a camera and increase an explosive payload. After this research it is possible to order the needed or recommended components and assemble the UAS.

3.2.2 Attaching explosives to UAV platform

Off-the-shelf UAVs usually have more power than it is needed for flight. Because of this the UAVs gain better flight performance and they are more

[13] In the most known e-shop in the Czech Republic.

attractive for the customers. So why not to utilize this fact and attach an explosive or a grenade to a UAV? This tactic was used by some extremist groups during the fights in Syria. Members of these groups attached grenades, mortar's ammunition or other explosives and dropped them with high accuracy thanks to a camera targeting [20].

The author conducted very simple experiment with 'obsolete' DJI Phantom 4 Pro [21]. A cargo of 350 g was attached to the UAV with weight of 1388 g and the UAV took off without any problems. But the not well-designed shape of the cargo caused minor problems with manoeuvrability during the flight and serious problems during landing. Control electronics was not able to deal with moved centre of mass. But landing is not the biggest issue during the 'suicide' or 'bombing' types of UAV attack. Some other sources, e. g. [22] presents safe payload weight about 462 g (1.02 lbs.) for DJI Phantom 4 Pro.

4 DETECTION AND IDENTIFICATION OF UAVS

Fully automated detection and identification is very complicated issue at the present state of art. Because of it, in the article it will be discussed detection and identification made by sensor's operators, or done in the integrated UAS protection solution. Any complex protection system against small UASs must be strictly modular, to allow easily upgrade individual parts and to improve detection capabilities.

The DJI company can offer a device that is capable of detect and identify most of the commercially available UAS [23]. The device uses a knowledge of the communication protocol used by UAS created by this company. The manufacturer presents an arbitrary range up to 50 km in stationary deployment and identification time from 2 seconds.

Types of sensors, which can be used for UAS detection and identification will be discussed in the next section.

4.1 Radar

Radar represents proven type of detection large flying objects. Various wavelengths were tested during time and now it is possible to manufacture a radar capable of small objects detection, with reflection surface just hundredths of square meter. In [3] was conducted a laboratory and field experiment with very interesting results. It is very unfortune, that most of these results are very sensitive and were not published by the authors.

Radar is best for long range detection, up to 30 km. Various manufacturers presents these instrumental ranges usually more optimistic than the real results.

However, this way of detection is not always precise and false detections may occur time to time. The reason is the size of a small UAV is very close to the size of larger birds.

4.2 Radio

Radio wave detection is relatively easy. The following radio spectrum analysis as well. Unlicensed Wi-Fi bands at 2.4 GHz or 5.6 GHz are used for commercial UAVs control. The communication is done by various protocols. A communication protocol of LTE mobile networks is very often used, but in the unlicensed Wi-Fi bands. It is because of its jamming resistance and better transmission properties than classical Wi-Fi protocol.

Off-the-shelf and racing UAVs are not usually autonomous and they use 2 radio channels. One for control signals and telemetry and the other with wider bandwidth for video stream from a digital camera attached to the UAV. This fact allows to detect and target the control station of UAS.

Identification of the UAS can be a problem. Operator has to analyse collected data from the control and telemetry channels, which is almost impossible in real-time.

4.3 Optics

UAVs automatic detection with digital cameras is great challenge for the image analysis specialists. At the time there are several systems, which declare an ability to detect a UAV in the field of view of the camera in the very few seconds. But these systems are not enough reliable and they are quite expensive.

More suitable approach of using optical sensors is using them for detection confirmation of other types of sensors. This confirmation can be easily and cheaply done by an operator. It is very easy to install a remote-controlled rotatable mast with set of cameras. The mast can be semi-automated controlled by the control system and an operator. The control system points the camera based on the information from other sensors and operator can adjust the parameters and then confirms the detection of a UAV. It is also possible to use the mast without connection to any sensors and to be controlled only by the operator.

It is not necessary to use only stationary cameras installation on the masts. Portable cameras equipped with GPS and laser range-meter can be connected to the command and control system and they can provide reliable detections as well.

4.4 Acoustics

Success rate of an acoustic detection depends on the area, where this type of sensor will be used. It is possible to detect UAVs with network of microphones, because of the limited range of this type of sensor. Yet microphones can be very cheap and easy to use.

It is also possible to use audio sensors to identify specific type of UAV [24] discussed possibility of using the Linear predictive coding (LPC) for UAVs detection and identification. The LPC uses sound samples and creates a numeral representation of the sound signature. It is possible to distinguish various types of sound sources, such as a truck, a gun shot or certain types of UAVs. But all of this is limited by the range of an acoustic sensor and its surroundings. Defence can contain many cheap sound collectors, but it should not be the only way of detecting UAVs.

5 ELIMINATION

UAV elimination is the last phase of the whole UAS defence. There are basically two ways of UAV elimination: Lethal and non-lethal with jamming. Both ways have their pros and cons, so there is no all-time right way of UAV elimination.

5.1 Non-lethal elimination

Non-lethal elimination is done by jamming radio control channel or by spoofing the positional data.

An interesting way of protecting the Russian president Vladimir Putin appeared recently. Russian security service uses GPS spoofing at places, where the president occurs. A non-profit organization C4ADS from the USA discovered from public data, that ships from certain waters moved to a land airfield approximately 200 km from the sea. This strange ship movement was done by transmitting false GPS coordinates which corresponds to the coordinates of nearby airfields to deceive commercial UAVs position restrictive systems. Because most of the manufacturers put into their UAVs restricted areas, the UAV is not able to fly in the area.

This way of protection can be effective against commercial UAVs, but it is ineffective against professional military UAVs with inertial navigation.

The GPS spoofing can also be very dangerous for any civilian GPS users. Many systems and people rely or even depend on the accurate position and time from GPS. In the piece time this type of protection can do more harm than good, especially in the Central Europe.

Decipherment of UAS's communication protocol and following take over can be another way of UAV elimination. This approach itself is on the edge of the law, because you have to decode a communication protocol with reverse engineering, which can be a violation of the EULA[14]. Big number of manufacturers and incompatibility between various UASs represents another disadvantage of this approach. Additionally, communication protocols change and evolve during time, so there is a time lack between launching a new UAS and gaining an ability to take over this new UAS.

Last conventional way is jamming the whole radio spectrum used for control channel. This is again usable only for a certain category of UASs. Again, it is on the edge of the law[15]. But this can be a way, how to eliminate unwanted UAVs from the protected area.

Big advantage of using a non-lethal elimination is the fact, that it can be used in densely populated areas, including cramped spaces in the cities. Lost of the UAV's control or fall of the UAV can only do any damage to the public or private property or harming people.

5.2 Lethal elimination

Lethal elimination is an ordinary usage of brute force to end a flight of the UAV. The best way is by damaging or destroying rotor blades. Only a slight damage can make worse the flight characteristics and manoeuvrability. The most suitable for this is using shotguns with many projectiles. This rises the probability of hitting a rotor blade. An experienced shooter should be able to hit a UAV flying at low altitude.

Using firearms at peace time is very controversial. Especially in the densely populated areas. A risk of collateral damage to a public property or human lives is too high there. So, this is the reason, why using firearms should be permitted only on very special cases and not in the cities or populated areas.

6 CONCLUSION

Protection of any area against small UAVs is very complex task. There is no "silver bullet" which will protect any possible area. It is necessary not only reflect the specifics of the protected area during the defence planning process, but it is vital to define the UAV threat type to which the defence should be effective.

A defence against small UAVs would have very different characteristics than defence against professional military UAVs, or swarms of these UAVs. This article focused on a single, or small number of UAVs, not swarms of cooperating UAVs.

The type of attack is also very important to decide. Should be the defence effective only against directly attacking UAVs with firearms or explosives, or even against an information collecting UAVs? Should be effective against high flying UAVs or low flying UAVs? These questions determine sensors and effectors usage.

Next question should be the assumed amount of losses during a successful attack. As a successful attack can be considered also a collecting and mining the information, especially on soft targets. These

[14] End-User License Agreement.

[15] Czech telecommunication office, the radio spectrum authority in the Czech Republic, would not be pleased, if the unlicensed band is being jammed for any time.

targets can be attacked with bigger impact after profound reconnaissance. This again affects the types of sensors and their quantity.

Another variable is concrete surroundings and ability to choose an elimination method. It is hard to say, which of the presented ways is less complicated or doable. Each of the approaches has its advantages. Using firearms is very limiting in populated areas, so they should be used only in uninhabited areas. If the UAV would quickly manoeuvre and the firearm operator would not be careful enough, there is very high risk of damaging the surroundings or harming any nearby people.

The primary task is detection using multispectral, multilevel, multimodal, and multisensory strategy in a fight against small UAS. The effective basis for the UAV detection is the multisource data fusion. The modelling and simulation are the often-used research methods, how to prepare and design any counter UAV protection and should be used for validating the design before building any defence system.

References

[1] Řízení letového provozu ČR: *Doplněk X – Bezpilotní systémy* [online]. [cit. 26. 4. 2019] Available at: https://aim.rlp.cz/predpisy/predpisy/dokumenty/L/L-2/data/effective/doplX.pdf

[2] NOVÁK, V.: *Předpisy pro létání s drony v ČR*. [online] [cit. 26. 4. 2019] Available at: http://www.droneweb.cz/legislativa-provozu-dronu/item/37-predpisy-pro-letani-s-drony-v-cr

[3] FARLÍK, J., KRÁTKÝ, M., CASAR, J., STARÝ V.: *Multispectral Detection of Commercial Aerial Vehicles.* Sensors (Basel, Switzerland), 19(7), 1517. doi:10.3390/s19071517, pages 1–28. Available online at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6480366/pdf/sensors-19-01517.pdf

[4] KRÁTKÝ, M., FARLÍK, J.: *Countering UAVs – the mover of research in military technology.* Defence Science Journal. 68. 460-466. 10.14429/dsj.68.12442.

[5] TIAN, Y., WANG, Z., HIANG, Q.: *UAV Remote Control Signal Analysis based on GNU Radio and USRP X310.* Pages 2502-2506. 10.1109/IMCEC.2018.8469271.

[6] DAVIES, G., HORTON, H., JOSHI, A.: *Gatwick Drone Chaos Continues into a Third Day.* [online] [cit. 26. 4. 2019] 2018. Available at https://www.telegraph.co.uk/news/2018/12/20/gatwick-chaos-drones-cause-flights-cancelled-live-updates/.

[7] WELLING, P., SPEIRS, P., SCHUEPBACH, C., BOENIGER, U., PRATISTO, H.: *Radar systems and challenges for C-UAV.* 2018 19th International Radar Symposium (IRS), Bonn, 2018, pp. 1-8. Online ISBN: 978-3-7369-9545-1.

[8] SOSNOWSKI, T., BIESZCZAD, G., MADURA, H., KASTEK, M..: *Thermovision system for flying objects detection.* 2018 Baltic URSI Symposium (URSI), Poznan, 2018, pp. 141-144. Online ISBN: 978-8-3949-4213-7.

[9] PROIETTI, P., GOLDIEZ, B., FARLÍK, J., Di MARCO, B.: *Modelling and simulation to support the counter drone operations (NMSG-154).* Lecture Notes in Computer Science 10726, 2018. Pages 268–284. Online ISBN: 978-3-319-76072-8.

[10] BOUVRY, P., CHAUMETTE, S., DANOY, G. ROSALIE, M. SANDER, J.: *Using heterogeneous multilevel swarms of UAVs and high-level data fusion to support situation management in surveillance scenarios.* 2016 IEEE International Conference on Multisensor Fusion and Integration for Intelligent Systems (MFI), Baden-Baden, 2016, pp. 424-429. Doi: 10.1109/MFI.2016.7849525. Electronic ISBN: 978-1-4673-9708-7.

[11] JOHN, R.: *Dron Phoenix: Pseudosatelit s neomezenou délkou letu.* [online] [cit. 7. 5. 2019]. Available at: https://www.armadninoviny.cz/dron-neomezenou-delkou-letu.html.

[12] *Geo zone map.* [online] [cit. 7. 5. 2019]. Available at: https://www.dji.com/cz/flysafe/geo-map.

[13] *DRON SYMA X5SW PRO.* [online] [cit. 7. 5. 2019]. Available at: https://www.rcprofi. cz/poradna/srovnani-verzi-dronu-syma-x5c.

[14] *Srovnání jednotlivých verzí dronu SYMA X5C.* [online] [cit. 7. 5. 2019]. Available at: https://www.rcprofi.cz/poradna/srovnani-verzi-dronu-syma-x5c

[15] *DJI Mavic 2 Enterprise (DUAL) Universal Edition.* [online] [cit. 7. 5. 2019]. Available at: https://www.alza.cz/dji-mavic-2-enterprise-dual-universal-edition-d5548224.htm.

[16] *Mavic 2 Enterprise.* [online] [cit. 7. 5. 2019]. Available at: https://www.dji.com/cz/mavic-2-enterprise

[17] *How to build a drone|Step by step guide.* [online] [cit. 25. 5. 2019] Available at: http://dronenodes.com/how-to-build-a-drone/.

[18] CARTER, J.: *How to build your own drone for $99.* [online] [cit. 25. 5. 2019]. Available at: https://thedronegirl.com/2018/05/06/build-your-own-drone/.

[19] *xcopterCalc – Multicopter Calculator.* [online] [cit. 25. 5 2019], Available at: https://www.ecalc.ch/xcoptercalc.php.

[20] GIBBONS-NEFF, T.: *ISIS drones are attacking U.S. troops and disrupting airstrikes in Raqqa, officials say.* [online] [cit. 25. 5. 2019]. Available at: https://www.washingtonpost.com/news/checkpoint/wp/2017/06/14/isis-drones-are-attacking-u-s-troops-and-disrupting-airstrikes-in-raqqa-officials-say/

[21] DJI: *Phantom 4 Pro.* [online] [cit. 25. 5. 2019] Available at https://www.dji.com/cz/phantom-4-pro.

[22] Dronethusiast.: *5 best heavy lift drones [2019]-large drones that have high lift capacity.* [online] [cit. 25. 5. 2019] Available at: https://www.dronethusiast.com/heavy-lift-drones/

[23] *DJI Aeroscope.* [online] [cit. 26. 4. 2019], Available at: https://www.dji.com/cz/aeroscope.

[24] VILÍMEK, J. BUŘITA, L.: *Ways for copter drone acustic detection.* ICMT 2017, pages 349-353. Online ISBN: 978-1-5090-5666-8.

Mgr. Jakub **VILÍMEK**
CIS Department
University of Defence Brno
and URC Systems Brno
Kounicova 65
662 10 Brno
Czech Republic
E-mail: jakub.vilimek@urc-systems.cz

Jakub VILÍMEK - is a software developer in the company URC Systems in Brno. He is a Ph.D. Candidate of the Faculty of Military Technology at University of Defence in Brno. His dissertation thesis is focused on planning defence system against the small UAV threats. He was part of the solvers team for the project SIMULEB - Simulator of command and control systems radio networks of defined combined brigade units for EW units training. The main aim of this project was to develop the SW tools for training of CZE Army EW specialists which includes SW simulator for modeling of "clasical" and sophisticated radio networks and communications of the combined task forces up to brigade level.