The Sky is Falling Down: Unmanned Aerial Vehicles as Emerging and Disruptive Technology Threat Assessment

Evangelos Mantas **Constantinos Patsakis**
University of Piraeus
GREECE

emantas000@gmail.com kpatsak@unipi.gr

ABSTRACT

Unmanned Aerial Vehicles (UAVs), or commonly known as drones, have already proven their value in military operations both strategically and logistically efficient, becoming a significant asset to the modern-day military. Although medium-altitude long-endurance (MALE) UAVs are commonly used by armed forces throughout the world, small Unmanned Aerial Systems (sUAS) are used as well, in guerilla and urban warfare, making them extremely difficult to anticipate and eliminate in a timely manner.

The continuous decrease in the price of drones makes them available to numerous malicious actors, establishing them as the "new technicals" for the modern battlefield, posing a significant threat for the safety and success of an operation.

This work focuses on performing a specific threat assessment, using a UAV as an attack vector, that covers all aspects of a military operation. To this end, we first identify the threats against infrastructure, personnel and vehicles using drones as the main actor to stage an attack using a variety of sensors and payloads. Moreover, we determine the seriousness of the threat depending on the drone mission, developing intervention and mitigation plans that may protect or minimise the risk of loss against them. Finally, we discuss methods to assess the impact of opposing force's drones in military operations.

1. INTRODUCTION

As technology moves forward day by day, more challenges on the battlefield rise as well. A few years ago, advanced weapon systems were only available on a handful of military organisations. Today guerrilla or radical forces have access to market products that with a few modifications can prove quite efficient. Commercially available drones have been the platform of choice due to the tactical advantage they provide, their relatively low cost and flexibility to change the payload of the drone (e.g. cameras, weapons, sensors) depending on the mission. Hence the term "modern-day technicals", a term1 that goes back to the Somali civil conflict in the early 1990s where armed pick-up trucks relied on their speed and agility to launch assaults against enemy combatants. Modern-day armies already operate Medium-Altitude Long-Endurance2 (MALE) drones (e.g. MQ-9 Reaper3) that have the capability to reach an altitude between 25,000 and 50,000 feet and are capable of 24-hour missions, and High-altitude, long-endurance (HALE) drones (e.g. RQ-4 Global Hawk4) by contrast are typically capable of flying as high as 60,000 feet and can endure missions as long as 32 hours. Both these types of UAVs can inarguably offer a tactical superiority on the operational field.

Nonetheless, nowadays conflicts may take place in urban areas where warfare logistics are far more complex, take advantage of Small Unmanned Aerial Vehicles (sUAV) that can be easily and quickly deployed by guerilla/insurgents fighters and counter the technological superiority in the open battlefield through asymmetric capabilities5 in this restricted battlespace. Those sUAV's operate ISR (Intelligence, surveillance and reconnaissance) or strike missions and pose a new threat for the ground troops safety and operational success. Over the past few years, the Islamic State (ISIS) developed its own drone program

without any financial aid from a state actor, modifying already existing off-the-shelf commercial drones or making makeshift flying machines, providing detailed instructions and recommendations using social media to spread them online6 widely. Those drones have been modified to carry and deliver explosives to targets acting like flying Improvised Explosive Devices (IEDs). Since the beginning of the conflicts, the Islamic State fighters have increased their combat capabilities and experience in conducting drone missions and use social media to release propaganda material associated with the drone program. An International Center for the Study of Violent Extremism (ICSVE) research7 related to ISIS' drone activities within its territories in Syria, reveals that ISIS drone operations started during mid-January 2017 having established a training centre for the militants by March 2017 in the city of Raqqa. A modification and maintenance headquarters for drones and other digital equipment was set to a nearby location where the weaponisation of drones took place and later shipped them to a storage and distribution centre. Evidently, an adversary with a fully working logistics supply chain of weaponised drones is an immediate threat that endangers the success of an operation.

2. SCOPE OF WORK

The scope of this work is to shed some light on the use of drones in the context of military operations. More precisely, we try to answer the following questions:

- Who/What are the threats using a UAV as an attack vector?
- What are the implications against military assets?
- What can be done to minimise exposure to loss or damage?

We argue that in order to answer these questions, one has to identify the possible targets of the adversary, explore the threats that is exposed to, and assess the vulnerabilities that the adversary will try to exploit. Based on them, one can create a mitigation plan. This is summarised in Figure 1.

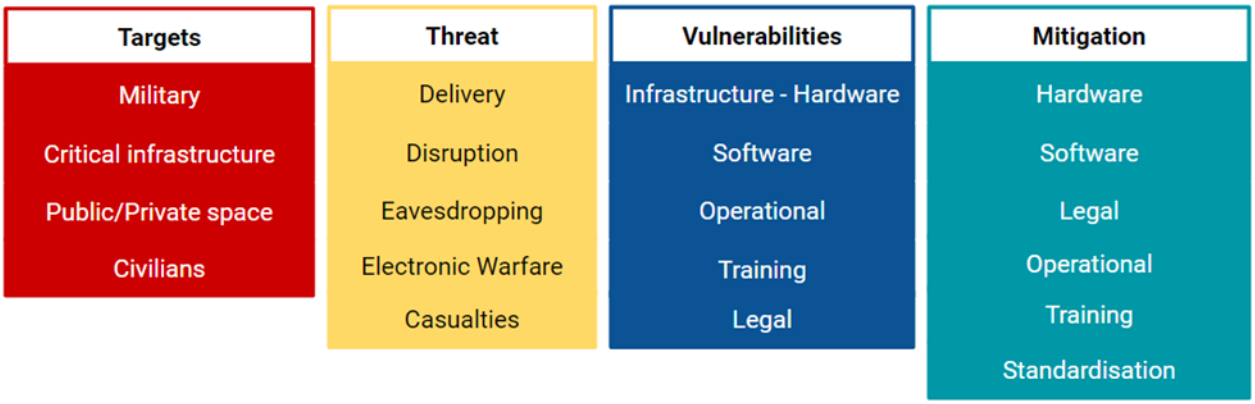

Figure 1: Threat assessment chart

3. THREAT IDENTIFICATION

In this section, we identify the threats that UAVs pose against different types of military assets, used as an attack vector in accordance with their operation.

Intelligence, Surveillance and Reconnaissance (ISR)

Intelligence is arguably one of the most critical components on the modern-day battlefield. Real-time

information on key infrastructures can provide the adversary with a tactical advantage. Drones equipped with high-resolution cameras can identify the location of facilities (e.g. administration buildings, armoury, barracks, gas stations, vehicle parks) and provide this information for a later attack using drones or other conventional strike methods (e.g. artillery/airstrike). Personnel and vehicles are also affected by the use of drones in ISR missions. Special forces operators already use state of the art drones1 to locate enemy combatants' location, but at the same time, adversaries use less sophisticated but quite efficient for the same purpose2 off-the-shelf commercial drones and should not be underestimated. Vehicles can also be affected by rogue drones' ISR capabilities, especially when moving in dense urban areas where mobility is limited, where they can be located to be ambushed by ground combatants using light weapons (e.g. machine guns) or RPGs and IEDs.

Drone Bombing

The technological advancement of drone technology has enhanced the operational capabilities of drones to carry a significant amount of payload from a range of sensors to explosive ordnance. For this reason, drones have emerged as a complex threat that is getting harder and harder to neutralise. Although the term "drone bombing" tends to associate western drone warfare with some form of targeted killing, in the context of gaining "full spectrum dominance10", the propaganda behind the drone usage of terrorist groups (e.g. ISIS), in contrast, does not similarly aim to establish them as a global dominant power. Terrorist organisations give extensive publicity to its use of armed drones, in a way that is probably meant as a demonstration for their tactical capabilities11 over the bigger and more sophisticated western drones. Over the last few years, numerous incidents have been reported of suicide drones used from rogue groups. The Aramco drone bombing incident in 201912 has shown the impact suicide drones have on against high-value infrastructure. Military bases are no exception whether they are located in conflict zones or in the domestic urban area of peacetime countries where the consequences of a drone attack on the personnel and the military logistics cycle would be dire. Armed drones could replace adversaries' mortar installations due to their precision and effectiveness to deliver a hit against ground personnel and vehicles. The threat of explosive-carrying drones is equal or even more severe to IEDs since the combination of IEDs and UAVs could be considered a significant evolution in offensive actions. A threat simulation study by NATO's CIED CoE in 201713 on the possible usage of drones from malicious actors accentuates the threat drones pose carrying a wide variety of ordnance from mortar shells to directional fragmentation charge, to name a few, and the impact of asymmetric and hybrid warfare scenarios on a fictitious simulated urban environment. The unsuccessful drone attack against Venezuela's President in Caracas in 201814 raises another awareness against high-value persons that cannot be overlooked. Country leaders, politicians, high ranking military officers and all sorts of public persons face another challenge during their public appearances that already existing security measures (e.g. area lockdown, roadblocks, marksmen in high locations) cannot anticipate, and their protection against these asymmetric and unexpected attacks seems more important than ever.

Electronic Warfare

Hostile actors may conduct "activities in cyberspace to cause harm by compromising communication, information, or other electronic systems, or the information that is stored, processed, or transmitted in these systems15" as described in Framework for Future Alliance Operations Manual. The lack of understanding of the ramifications of EW can have critical mission impact – even in the simplest possible scenario. A man-in-the-middle cyber-attack monitoring the communications or the control of autonomous systems can prove dire. Drones carrying electronic warfare ordnance can disrupt operational capabilities rendering communication systems useless endangering the safety of the ground operators and the operation's success. Although there are no reported cases of sUAV with such capabilities so far, with the current technological advancement, soon it may be the case. UAVs with the capability to deploy EW systems and sensors using the Joint Precision Airdrop Systems (JPADS) technology already exist as concepts16. Cybersecurity professionals have developed a drone that is capable of hacking devices16 to assess the cybersecurity resilience of companies and organisations during cybersecurity assessments. Nevertheless, vehicles and

aircraft with EW capabilities already exist, but they are harder to be utilised by terrorist groups since their cost of operation and maintenance is significant, and they require extensive training, but their threat should not be ignored.

			Impact			
			0 Acceptable	1 Tolerable	2 Unacceptable	3 Intolerable
			Little or No Effect	Effects are Felt but Not Critical	Serious Impact to Course of Action and Outcome	Could Result in Disasters
Likelihood	Improbable	Risk Unlikely to Occur			Electronic Warfare	
	Possible	Risk Will Likely Occur				
	Probable	Risk Will Occur				ISR, Drone Bombing

Figure: Proposed Threat Matrix

4. IDENTIFICATION OF VULNERABILITIES

Identifying the vulnerabilities of an organisation is critical since a malicious actor can exploit them. In what follows, we categorise key vulnerabilities in five diverse fields.

Infrastructure - Hardware

Key infrastructure and hardware are by default high-value targets, and their loss or defilement may cause serious damage and disruption of operational/critical services. Note that due to their extent, location, and other physical constraints, infrastructure and hardware may be an easy target for a drone.

Software

As technology advances, drones may prove more efficient in conducting Electronic Warfare. The software may also be targeted since it can control key infrastructure operations or services and should also be taken into consideration. The fact that a drone may approach a target can provide the adversary with the means to launch a cyber attack that could not be performed without physical presence as it may now use a wireless channel whose security can be compromised either through electronic means or intelligence.

Operational

The use of drones to conduct warfare is relatively new, and an organisation may not have an existing procedure to detect, identify and eliminate a drone in the nearby airspace. This operational insufficiency may be exploited by adversaries to attack key infrastructure, hardware and software.

Training

The potential lack of an established procedure may also indicate a potential lack in personnel training to handle incidents which can lead to serious casualties or injuries. Moreover, the improper handling of the drone may also impede the forensic investigation and attack attribution.

Legal

Different or not established legal frameworks of each country complicate the jurisdiction over actions against a drone attack. An adversary can exploit the legal gap to further hide her trails.

5. INTERDICTION AND MITIGATION PLAN

After identifying the attack vectors using drone, it becomes of main importance to interdict this threat. A proposed interdiction plan at a higher level consists of the following three steps:

- Detection of drone
- Identification of ally or hostile/Verification of intent
- Elimination/Mitigation of threat

UAV Detection Technology

Initially, to anticipate and eliminate the threat, enemy combatant drones must be identified. There are different methods to identify a drone with mixed results depending on the technology used, the environmental conditions and the technological advancement of the adversary drone. Visual identification without assistance (e.g. cameras with image processing identification algorithms) relies on the human factor (e.g. fatigue, visual capabilities) and may prove efficient only when the drone is at a close range and becomes extremely difficult at low light or during the night. For this reason, a more advanced approach is to be considered. Earlier research suggested software-assisted visual identification[17] and neural network classification[18] to identify and predict drones trajectory. Although the use of machine learning to detect drones has achieved great results, because of the small size of an sUAV this method is less robust. Other works focus on acoustic detection. In their work Nijim[19] et Al. propose an acoustic approach that identifies a drone by the humming sound frequency of the propellers during the flight. With the continuous development and evolution of drone technology, more advanced and efficient propellers emerge that generate less noise and therefore make detection more difficult. Taking into consideration the complexity of urban environments (e.g. unpredictable sound acoustics) audio detection has some limitations but provides good assistance to other detection methods. A combined method of visual and audio detection is proposed by Liu[20] et al., where a device with an array of cameras and microphones captures video feed and sound from all directions applied a detection algorithm that fuses video and audio features. According to the experimental results, a great accuracy improvement has been achieved, compared with the single-feature method (either video-only or audio-only) with over 80% success rate. Although the concept of using conventional radar may seem like a solution, the continuous transmission of signals to identify a drone may raise radiation health concerns. Moreover, another logistical problem is the high operating cost of a transmitter that works continuously. In their research, Liu[21]et Al. propose the use of passive radar as an alternative to conventional radar detection, which exploits existing infrastructure (e.g. TV-signal towers) as transmitters of opportunity with great

success in detecting small drones. Although this method can provide good intelligence on nearby flying drones in urban areas, it has some limitations as it requires an existing infrastructure and access to it, where it may not be the case in a combat area.

UAV Identification Technology

As technology advances, more drones are expected to occupy the airspace. Thus it is important to make a distinction between friendly and hostile drones. It would be catastrophic to cause damage or take out a friendly drone that serves a mission in the nearby area. Aircrafts and medium/long-endurance drones (MALE/HALE) already use a system known as Automatic Dependent Surveillance-Broadcast (ADS-B) which periodically transmits the aircraft position. Such technology could also be applied for small UAVs (sUAV), like the *remote ID*[22] that the FAA proposes and is expected to be launched in the near future. Although it is probable that malicious actors will fly their drones without such technology-enabled, drone identification technology could prevent the wrongful targeting and elimination of friendly drones.

Counter-UAV Capabilities

From ancient times till today, protection of military assets has been of main concern. Walls, outposts and armed guards may be the solution to conventional warfare, the use of drones to launch asymmetric attacks requires a new approach. Different types of Counter UAV (CUAV) measures are already available to provide a solution to this arising threat with "at least 235 counter-drone products either on the market or under active development[22]" exploiting a variety of techniques for detecting and/or intercepting drones. Below are presented some of the already existing CUAV technologies.

Drone Nets

Using nets to capture drones is currently one rising trend in CUAV capabilities. Drones that carry or shoot nets against small drones or static nets, can neutralise the threat in a safe manner since the rogue drone's propellers are tanged amongst the netting and come to a stop immediately. One significant advantage of this method is that the drone can be analysed by forensic experts, since it is still intact and provide more information about the mission, the flight path and the malicious actor location since it can be linked through the take-off point or the media (e.g. images, video) captured during the flight. One aspect that should not be forgotten is that in the event of an armed drone attack, it may endanger the infrastructure or the persons near the net or the drone with the hanging net.

Signal Jamming

Handheld jamming devices operate by emitting electromagnetic noise at the same frequencies the aircraft use for control communications and video transmission, disrupting its ability to receive any radio frequency (RF) command from the operator, triggering the drone's safety procedure, since they are programmed to land on the spot, or return back to the take-off point thus facilitating the tracking of the rogue operator, or the forensic analysis of the landed vehicle.

Electromagnetic Pulse (EMP)

Although the generation of high power Ultra Wide Band (UWD) EMP is difficult due to the technology available, a low power UWD EMP can still disrupt the operation of a drone[25] by incapacitating the onboard sensors. This kind of technology is yet to be proven effective in a real-life, non-simulated scenario.

Laser Strike

Platforms that exploit the electromagnetic spectrum to destroy the electronics of a drone or a swarm are

gaining popularity for their effectiveness and their near-infinite firing capacity. Such systems used to be much bigger in volume, but as technology advances, those systems can become smaller, and thus easier to be mounted on the ground or air vehicles.

Missile

Some would argue that anti-aircraft systems can already be used to neutralise those threats, but it is not the case. The recent event of using a $3.4 million Patriot missile to take out a hostile commercial-type drone[27], raises the issue of "efficiency vs economics". Drones should not be underestimated on their damage capabilities, but a more logistically feasible solution has to be found.

Conventional Weapons

Traditional firearms (e.g. shotguns, machine guns) may prove efficient in neutralising drones in close distance, but they are dangerous in causing collateral damage on nearby personnel.

Birds of Prey

Birds of prey have been used for hunting for thousands of years. Law enforcement agencies have used predator birds to take down drones but with low-efficiency results[28].

No-Fly Zones

Most commercial drones prevent the pilot from taking off in designated areas to protect critical infrastructure (e.g. airports, military bases, industrial plants) by adding the coordinates in the built-in autopilot of the drone. It must be noted although this safety measure minimises the risk of an accident by a *bona fide* pilot, this list can be relatively easily tampered with, thus providing no real protection against a determined adversary.

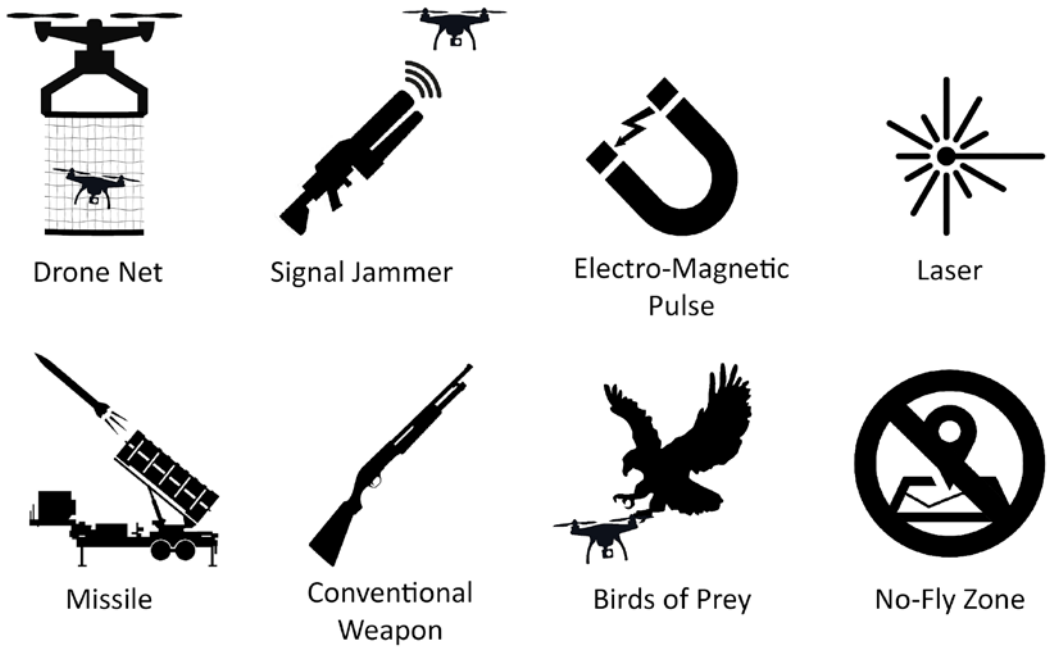

Figure: Available Interdiction/CUAV capabilities

6. EVALUATION PLAN

To properly assess the malicious drone impact against military assets, a proposed *purple teaming* evaluation scenario could take place, where the defence countermeasures will be tested to prove their effectiveness. Simply put, Red Team members will act as malicious actors using drones to emulate an attack against military assets. Simultaneously, the blue team is monitoring its systems, however, they cooperate to find measures that may improve the control or defeat the bypass. The aspects of the proposed evaluation plan contain a *Threat Emulation*, *Operational Impact*, and *Threat Mitigation.*

Threat Emulation

The purpose of the Threat Emulation is to challenge the full scope of the defences countermeasures described in the previous section, so that when an if a real attack the assets stay protected and the risk of failure in the military operation minimises. In the sector, *Threat Identification*, we identified the threats drones pose as an attack vector and those will determine the rules of engagement for the evaluation scenario. An example of this could be the following: "*A drone equipped with a camera locates areas of importance in an allied military base. After the drone unsuccessful elimination, a mortar strike hits the base, resulting in damages against infrastructure and soldier casualties"*. This scenario aims to determine the success of the countermeasures of the base.

Operational Impact

By definition, the operational impact is the effect of the disaster on an organisation's operation that determines the survival and continuity of the operation. The quantification of realistic impacts against a selected target, as described in the previous example may be variable, from loss of human life to financial damages due to the destruction of assets.

It is clear that establishing an evaluation plan is a complex and time-consuming procedure since there are a lot of key elements that have to be taken into consideration. This procedure differs depending on the military asset (e.g. infrastructure, personnel, vehicles) since there should be a different plan for each, but at the same time should be based on the same established principles of assessment.

7. CONCLUSIONS & OPEN ISSUES

As drones are expected to be widely used by adversaries to launch asymmetric and hybrid attacks, the importance to successfully interdict this emerging threat is becoming more imminent than ever. Nonetheless, there are many obstacles beyond the infrastructure solutions. For instance, the current legal framework has to be revised and amended to determine the fly zones for civilian drones and the jurisdiction clauses. Evidently, despite the need to monitor critical infrastructures which may span for kilometers (e.g. road infrastructure) it is not possible for the military in terms of resources to monitor the whole infrastructure and more over may not fall under its jurisdiction leading to many unnecessary problems in case it is deemed necessary to intervene. Beyond that, it should be understood that the operational framework, even for military personnel is not always well-defined since this is closely related to the training of the personnel. The latter is very important when personnel notices the presence of a drone in an area. Can they identify whether it is an ally or hostile? Due to the time criticality, who should be informed and how the personnel should act against it? Evidently, the answers do not have a simple yes/no form as the identification, contrary to face-to-face interactions are not so simple. Even if the above are tackled a standardisation of procedures and the drones per se is needed. While in the military one must always consider that the adversary will use ad hoc solutions, in order to maintain a fleet, several standards must be set. The continuous changes in the protocols, many of which not having proper cryptographic primitives, the introduction of new sensors and the use of new platforms to serve as the backbone of the drone impede their usage and investment on them as they imply a

continuous race to meet new software and hardware requirements. Moreover, this is introducing significant issues for the forensics as the tools, e.g. DROP[29], Gryphon[30], may not be relevant for different versions or drones. It should also be highlighted that there is no standard covering the aspects of forensics for drones to date. Notably, they cannot be considered as a computer or a mobile device to use, e.g. ISO17025, ISO/IEC 27037, NIST SP 800-86, NIST SP 800-202 processes. Such issues are going to be more and more relevant in the near future not only for the military as drone technology is here to stay and in most cases with a relatively low cost. Therefore, the establishment of baseline actions, processes and capacity building must be performed with a rather high priority.

8. ACKNOWLEDGMENT

We would like to thank DroneSec (https://dronesec.com/) for providing access to their Threat Intelligence platform of globally reported drone incidents.

9. REFERENCES

[1] https://www.geopolitica.info/technicals/

[2] https://defensesystems.com/articles/2015/05/27/uas-male-vs-hale-debate.aspx

[3] https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104470/mq-9-reaper/

[4] https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104516/rq-4-global-hawk/

[5] Khan, Umer. (2018). Urban Warfare.

[6] https://justpaste.it/jnabi7

[7] Almohammad, Asaad & Speckhard, Anne. (2017). ISIS Drones: Evolution, Leadership, Bases, Operations and Logistics. ICSVE Research Reports.

[8] https://www.cnet.com/news/heres-the-tiny-drone-the-us-army-just-purchased-for-soldiers/

[9] AlALAM, “Iraqi Army Targets ISIS Drone near Mosul,” ALALAM, October 03, 2016, http://en.alalam.ir/news/1868370

[10] Shaw, I., 2016. *Predator Empire*. Minneapolis (Minn.): University of Minnesota Press.

[11] Emil Archambault, Yannick Veilleux-Lepage, Drone imagery in Islamic State propaganda: flying like a state, International Affairs, Volume 96, Issue 4, July 2020, Pages 955–973.

[12] https://www.nytimes.com/2019/09/14/world/middleeast/saudi-arabia-refineries-drone-attack.html

[13] CIED CoE,(2017) C-UAV payload with IED. A LONG TERM SIMULATION BASED STUDY, North Atlantic Treaty Organization (NATO)

[14] https://www.nytimes.com/2018/08/10/world/americas/venezuela-video-analysis.html

[15] ACT,(2018) FRAMEWORK FOR FUTURE ALLIANCE OPERATIONS, North Atlantic Treaty Organization (NATO)

[16] O. Y. Tkachenko, "System of electronic warfare with UAVs," *2015 IEEE International Conference Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD)*, Kiev, 2015, pp. 324-327

[17] https://resources.bishopfox.com/resources/tools/drones-penetration-testers/attack-tools/

[18] N. Grammalidis, K. Dimitropoulos and T. Semertzidis, "Video and Signal Based Surveillance for Airport Applications," in *2013 10th IEEE International Conference on Advanced Video and Signal Based Surveillance*, Genova, Italy, 2009 pp. 170-175,doi: 10.1109/AVSS.2009.70

[19] A. Rozantsev, V. Lepetit and P. Fua, "Detecting Flying Objects Using a Single Moving Camera," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 39, no. 5, pp. 879-892, 1 May 2017, doi: 10.1109/TPAMI.2016.2564408.

[20] M. Nijim and N. Mantrawadi, "Drone classification and identification system by phenome analysis using data mining techniques," *2016 IEEE Symposium on Technologies for Homeland Security (HST)*, Waltham, MA, 2016, pp. 1-5, doi: 10.1109/THS.2016.7568949.

[21] H. Liu, Z. Wei, Y. Chen, J. Pan, L. Lin and Y. Ren, "Drone Detection Based on an Audio-Assisted Camera Array," *2017 IEEE Third International Conference on Multimedia Big Data (BigMM)*, Laguna Hills, CA, 2017, pp. 402-406, doi: 10.1109/BigMM.2017.57.

[22] Y. Liu, X. Wan, H. Tang, J. Yi, Y. Cheng and X. Zhang, "Digital television based passive bistatic radar system for drone detection," 2017 IEEE Radar Conference (RadarConf), Seattle, WA, 2017, pp. 1493-1497, doi: 10.1109/RADAR.2017.7944443.

[23] https://www.faa.gov/uas/research_development/remote_id/

[24] Holland Michel, Arthur. “Counter-Drone Systems.” Center for the Study of the Drone at Bard

[25] K. Yu Sakharov, A. V. Sukhov, V. L. Ugolev and Y. M. Gurevich, "Study of UWB Electromagnetic Pulse Impact on Commercial Unmanned Aerial Vehicle," *2018 International Symposium on Electromagnetic Compatibility (EMC EUROPE)*, Amsterdam, 2018, pp. 40-43, doi: 10.1109/EMCEurope.2018.8484992.

[26] https://www.raytheonmissilesanddefense.com/news/feature/beam-on

[27] https://www.theverge.com/2017/3/16/14944256/patriot-missile-shot-down-consumer-drone-us-military

[28] https://www.theverge.com/2017/12/12/16767000/police-netherlands-eagles-rogue-drones

[29] Clark, Devon & Meffert, Christopher & Baggili, Ibrahim & Breitinger, Frank. (2017). DROP (DRone Open source Parser) your drone: Forensic analysis of the DJI Phantom III. Digital Investigation. 22. S3-S14. 10.1016/j.diin.2017.06.013

[30] Mantas E., Patsakis C. (2019) GRYPHON: Drone Forensics in Dataflash and Telemetry Logs. In: Attrapadung N., Yagi T. (eds) Advances in Information and Computer Security. IWSEC 2019. Lecture Notes in Computer Science, vol 11689. Springer, Cham. http://doi-org-443.webvpn.fjmu.edu.cn/10.1007/978-3-030-26834-3_22