MSc THESIS

Cybersecurity Risks Posed by Unmanned Aircraft Systems

Student: Moustakas Dimitrios
SID: P3341811

Supervisor

Professor Dimitris Gritzalis

Date: September 2020

The undersigned have examined the thesis entitled "**Cybersecurity Risks Posed by Unmanned Aircraft Systems"** presented by **Dimitrios Moustakas**, a candidate for the degree of **Master of Science In Information Systems** and hereby certify that it is worthy of acceptance.

_____ _____

Date Dr. Dimitris Gritzalis

_____ _____

Date Dr. George Stergiopoulos

_____ _____

Date Dr. Theodoros Ntouskas

Abstract

Unmanned Aircraft Systems (UAS) are yet another marvelous technological achievement. They gave men the ability to fly and see from the eyes of a bird, and in an instant what was known for the cybersecurity became obsolete. The abilities of Unmanned Aircraft Vehicles (UAV) have sharply improved in the recent years, while simultaneously their cost and simplicity to use have steadily declined. Moreover, those improved capabilities have led to the adaption of UASs as a medium for a plethora of commercial and civilian usages.

Those drastic improvements of the drones' abilities made them an ideal tool for malicious cyber-related acts. Critical infrastructures must adapt in this new era and threat with suitable cyber-defenses, anti-drone measures, risk management and constantly re-evaluate their plans.

The aim of this thesis is the analysis and presentation of cybersecurity risks which unmanned aircraft systems pose and how their threat capabilities should pave the way in risk assessments of every modern critical infrastructure. Each technological and cyber-criminal related aspect of drones is analyzed along with presentation of various cases where drones were used for cyber-attacks. With the aim of holistic approach, this thesis presents a number of anti-drone platforms and technologies. Based on the aforementioned, two realistic attack scenarios are presented and introduced along their corresponding countermeasures. Last but not least an anti-drone oriented action plan is introduced along with comments and suggestions.

Keywords

Unmanned Aircraft Vehicles (UAV), Unmanned Aircraft Systems (UAS), cybersecurity, drones, IoT, Artificial intelligence, smart airports, critical infrastructures, swarm logic, industrial espionage, Wi-Fi mapping, 3D mapping.

Περίληψη

Τα συστήματα μη επανδρωμένων αεροσκαφών (UAS) αποτελούν ένα ακόμα αξιοθαύμαστο τεχνολογικό επίτευγμα. Έδωσαν στους ανθρώπους τη δυνατότητα να πετούν και να βλέπουν μέσα από τα μάτια ενός πουλιού, καθιστώντας πλέον τα περισσότερα σχέδια κυβερνοάμυνας ως παρωχημένα. Οι ικανότητες των μη επανδρωμένων αεροσκαφών (UAV) έχουν βελτιωθεί σημαντικά τα τελευταία χρόνια, ενώ ταυτόχρονα το κόστος και η απλότητα στη χρήση τους μειώνονται με σταθερό ρυθμό. Παράλληλα, αυτή η βελτίωση στις δυνατότητες τους, οδήγησε στην υιοθέτηση των UAS ως μέσο μιας πληθώρας εμπορικών και ιδιωτικών χρήσεων.

Αυτές οι δραστικές βελτιώσεις στις ικανότητες των UAV, δημιούργησαν μια ιδανική πλατφόρμα για την ενορχήστρωση κακόβουλων κυβερνοεπιθέσεων. Βάση αυτών κρίνεται αναγκαία η προσαρμογή των κρίσιμων υποδομών με σκοπό την αντιμετώπιση των νέων απειλών, μέσω κατάλληλων μέτρων κυβερνοάμυνας, λήψη αντίμετρων εναντίον των UAV, νέα σχέδια διαχείρισης κίνδυνου, αλλά και η διαρκής ενημέρωσή τους. Ο στόχος της παρούσας διπλωματικής εργασίας είναι η ανάλυση και παρουσίαση των κινδύνων κυβερνοασφάλειας που μπορεί να προκληθούν από τη κακόβουλη χρήση μη επανδρωμένων αεροσκαφών, και πώς οι ικανότητες τους, και η απειλή που συνιστούν, θα πρέπει να ορίζουν την πολιτική ανάλυσης κινδύνου κάθε σύγχρονης κρίσιμης υποδομής.

Στην έκταση της παρούσας εργασίας, αναλύεται κάθε τεχνολογική πτυχή των UAV η οποία σχετίζεται με κυβερνο-επιθέσεις, ακολουθουμένη από τη παρουσίαση διαφόρων περιπτώσεων στις οποίες UAV χρησιμοποιήθηκαν ως μέσα για την διεξαγωγή κυβερνο-επιθέσεων. Με σκοπό την ολιστική προσέγγιση του θέματος, περιλήφθηκαν κεφάλαια τα οποία παρουσιάζουν και αναλύουν μια σειρά από πλατφόρμες και τεχνολογίες που στοχεύουν στην αντιμετώπιση των UAV. Με βάση τα προαναφερθέντα, θα παρουσιαστούν δύο ρεαλιστικά σενάρια κυβερνο-επίθεσης, συνοδευόμενα από προτεινόμενα αντίμετρα για την εξουδετέρωση τους. Τέλος, παρουσιάζεται ένα σχέδιο δράσης με στόχο την επιτυχή κυβερνο-άμυνα κρίσιμων υποδομών εναντίον των UAV, μαζί με σχόλια και προτάσεις.

Λέξεις – κλειδιά

Μη επανδρωμένα εναέρια οχήματα (UAV), μη επανδρωμένα εναέρια συστήματα (UAS), ασφάλεια στον κυβερνοχώρο, drones, διαδίκτυο των πραγμάτων, τεχνητή νοημοσύνη, έξυπνα αεροδρόμια, κρίσιμες υποδομές, λογική σμήνους, βιομηχανική κατασκοπεία, χαρτογράφηση ασύρματου δικτύου, τρισδιάστατη χαρτογράφηση.

Table of Content

Table of Figures

Cybersecurity Risks Posed by Unmanned Aircraft Systems

MSc THESIS

1 Introduction

1.1 Intro

The implementation of Unmanned Aircraft Systems (UAS) has created an abundance of new abilities and evolution paths in many fields of human society. UAS enabled humans to collect or project information from ideal aerial positions, both aspects can be easily exploit for malicious acts, hence creating a whole new chapter in the field of cybersecurity.

In the United States, as of 2019, the registered drones alone are more than 2 million, while it is estimated by Federal Aviation Association (FAA) of United States that by the end of 2020 the actual number of drones is expected to grow exponentially, well over passing 7 million drones just in Unites States. Numbers which are far greater if we take into account the unregistered drones. Those huge numbers reflect two facts regarding the use and exploitation of unmanned aircraft systems such as drones: Firstly, the people are becoming increasingly accustomed with the existence of such equipment in their vicinity, facilitating the use of unmanned aircraft systems in the aviation sector. Secondly, the general availability of such equipment to the public, most of the times anonymously, creates risks and concerns regarding their use, since the usage of drones and UAS only for non hazardous mission and services cannot not be ensured.

Starting from the risk and hazards that unmanned aircraft systems may possess, it is undoubtedly a fact that each and every cyber-service which is currently provided globally may be affected at some level from the malicious use of UAS [1-2], [38-40]. Furthermore, large scale critical infrastructures can be threatened more easily from the use of UAS, since the large geographical space which they are consisted of, complicates the task of monitoring the airspace. The small size of UAS makes it harder to detect and offers access

to the culprit to otherwise well guarded infrastructure of the organization. Fences and physical barriers along of the organization premises, offer little to no protection, since their construction and maintenance for covering such area is tremendously costly. Worth mentioning is that such an installation of fences would also affect negatively the psychology of the working force of the company along with the negatively publication from such a installation around the premises of the company.

The technological evolution described above, has paved the way for a new era in terms of service provided and lurking cybersecurity risks, both in unparalleled till now levels.

1.2 Rationale

The technological advancement which has taken place in the last decade has lead to a tremendous increase in the capabilities and popularity of unmanned aircraft vehicles and in spite of the plethora of research which has been done from the aspect of cybersecurity and UASs, there are still many threats and risks which have to be analyzed. The commercially available drones will continue to advance in parallel with the technology of 21th century and cyber-physical attacks based on UAVs as a platform can cause major damage to services and critical infrastructures [3-4]. Moreover, UAVs liabilities have created the perfect background for cyber-attacks which target the UAVs itself, so that they can be used in subsequent attacks against critical infrastructures [7-9].

Based on the aforementioned and fueled by my interests in UAVs and cybersecurity, I hereby present in this thesis a holistic approach on the cybersecurity threats which both critical infrastructures and UAVs have to face.

1.3 Structure

In the initial chapters of the thesis, a state of the art review on the unmanned aircraft systems (UAS), their history, evolution, liabilities and capabilities are presented, accompanied by a technical and theoretical analysis of cyber-attacks which can be utilized through the adaptation of UAS.

A further analysis and categorization of the above methods and techniques follows, analyzing vital aspects of the connection of UAS and cybersecurity. More specifically the

use of commercial available drones as means for industrial and public espionage, the cybersecurity risks and liabilities that the integration of RFID creates, Wi-Fi mapping and Swarm logic are presented along with the cybersecurity impact which drones can inflict in internet of things based technologies and critical infrastructures.

Following the aforementioned chapters, the UAS security challenges which every modern critical infrastructure is burdened with are analyzed, accompanied by a specialization in airports cybersecurity and evaluation results.

2 State of the art

During the recent years, many studies and researches have been published regarding the unmanned aircraft vehicles, the threats they pose, the use of artificial intelligence with UAVs and the impact which they may inflict in a critical infrastructure. Based on the aforementioned, this thesis will try to collect and fuse all this information in order to create the proper knowledge for the cybersecurity threats posed by UAS and their utilization in the aviation sector.

2.1 Unmanned Aircraft Vehicles and cybersecurity threats

Cyber-physical attacks were a plausible concern in the past decades, but during the latest years they became a threatening reality. More precisely, the term "cyber-physical attack" refers to malicious acts in the cyber-space which have as a result physical impacts [1]. As the technology enables an increasing number of sensors, metrics and controls to be used and connected to the web, it also enables the malicious control over those vital equipment and information. By conducting a cyber-physical attack, a hacker is able to control the water pumps of dam or the medical equipment in a hospital.

Even more disturbing is the idea that this kind of attacks can occur in situations that were unthinkable till recently. A cybersecurity company "Pen Test Partners", proved theoretically that a hacker can take control of the ballast tank of cargo ships, with catastrophic results [2].

Figure 1: Hoegh Osaka capsized ship due to the fact that ballast tanks weren't properly filled and the load hadn't been correctly assessed [2]

Ballast tanks are vessels that regulate the buoyancy of a ship by filing or emptying up with water. Those tanks are now controlled and monitored by sensors and pumps connected to the internal net grid of the ship.

According to the research, an out of date firmware is enough to enable access to that grid through a wireless controller or a default setting Moxa device server. Though such kinds of attacks require technical skills and knowledge regarding the controls and the functions of a ship, the malicious act of hacking and applying those, requires half-decent knowledge of networks and cyber-attacks. Furthermore, the research claims that the same malicious act can be done with the same convenience against the autopilot of the ship, resulting in a hazardous situation [2].

This entire scenario is based on the fact that the internet of things made possible to access easily that kind of infrastructures and conduct a cyber-physical attack. Vital infrastructures security relies on the fact that their network and access point will be out of reach of such attacks, due to the geographical distance of the equipment from the attacker. An unmanned aircraft system can easily overpass those kind of defenses and expose the internal network of the infrastructure to a hacker [3].A group of security experts at the Praetorian firm [4], decided to test and prove that the above statement was entirely possible and relatively easy to accomplish.

Figure 2: According to the paper, 1600 unique internet of things devices have been uncovered during their experiment, 453 of them are made by Sony, and 110 by Philips. [4]

Their research took of advantage of the ZigBee communication protocol, which is often used as communication link for internet of things devices. They equipped their drone with antennas able to sniff and capture the messages sent with the use of the mentioned software. Furthermore it is able to connect with the devises using this protocol and through the use of an integrated GPS system, it is able locate the device position with relative preciseness.

The above papers do not directly confront the use of unmanned aircraft system for undertaking malicious acts, rather exploiting and analyzing individual pathogens and usages of systems and drones. This thesis will exploit the already provided information in order to combine the picture of such an attack carried out by a hacker.

According to the researcher and security expert Glenn Wilkinson [5] [6], drones can also be used to monitor and record detail network information of smart phones and access points. In 2014, at the Black Hat security conference in Singapore, Glenn Wilkinson stated and proved that this kind of knowledge can easily be used for malicious acts [6]. More precisely, the article and paper refer to the creation and abilities of Snoopy-drone. A drone which incorporates the Black Hat software called “snoopy” in order to monitor the wireless signals in the vicinity along with the geographical location of the source of each signal [5].

By gathering network information an attacker is able to impersonate a device like an access control or a Wi-Fi router. This cyber-attack known as “karma-attack”, uses the unique identification of network devices in order to disguise the drone as the safe network to which the smart phone usually connects to. When the user starts accessing his network accounts, the Snooby software steals and records his credentials. By doing so, an attacker is able to gain access to sensitive information like social media passwords, email password, credit card number or even the credentials used to regulate a pacemaker [6].

While this paper reveals security threats from the use of such malicious software to drones, it does not address the problem from the aspect of cyber-defense against those threats. Moreover, it does not refer to whole infrastructures like hospitals and airports and the magnitude of the problem that such a cyber-attack can inflict.

The UAV threats are not restricted to only cyber-physical attacks and data stealing, rather they can expand to terrorist attacks [7]. According to Donna.A.Dulo, a drone can be easily used for malicious acts, which surpass the imagination and threaten the very reality of

western civilization.He states that a rogue drone or even worse, a number drones can be used in order to physically attack a critical infrastructure in the aviation sector. In other words, they can be used to attack radar installation and disrupt the function of the entirety of the airport. Furthermore, those drones can also be used as a weapon against the engines of the airplanes itself and inflict countless casualties or even used as projectiles against bypassing pedestrians.

2.2 Cybersecurity liabilities of Unmanned Aircraft Vehicles (UAV).

Following the threats posed by an unmanned aircraft vehicle, it is becoming clear that some of the measures regarding the cybersecurity of critical infrastructure against UAVs should be taken to the cyber-defense of the UAV itself.. Moreover, the UAV industry itself has taken measures regarding cyber-attacks and has incorporated some solutions in the form of updates or with the creation of new, safer models.

According to the paper of Krishna, C. and Murphy, R "A Review on Cybersecurity Vulnerabilities for Unmanned Aerial Vehicles" [8], although the number of attacks were not so many, they have clearly shown the high number of liability issues present in the cybersecurity of drones. The study goes as far as categorizing the attacks based on the type of the exploitation. The most worth to mention categories are named below, while their terms and definitions are going to be extensively analyzed in the following chapters of this thesis:

- The ones targeting the GPS function of the UAV, either by spoofing or by jamming [8].

- Those targeting the control communications stream like a deauthentication attack and zero-day vulnerabilities attack.

- Attacks which have as a target the data communications stream, either by intercepting the data feed or by executing a zero-video-replay-attack.

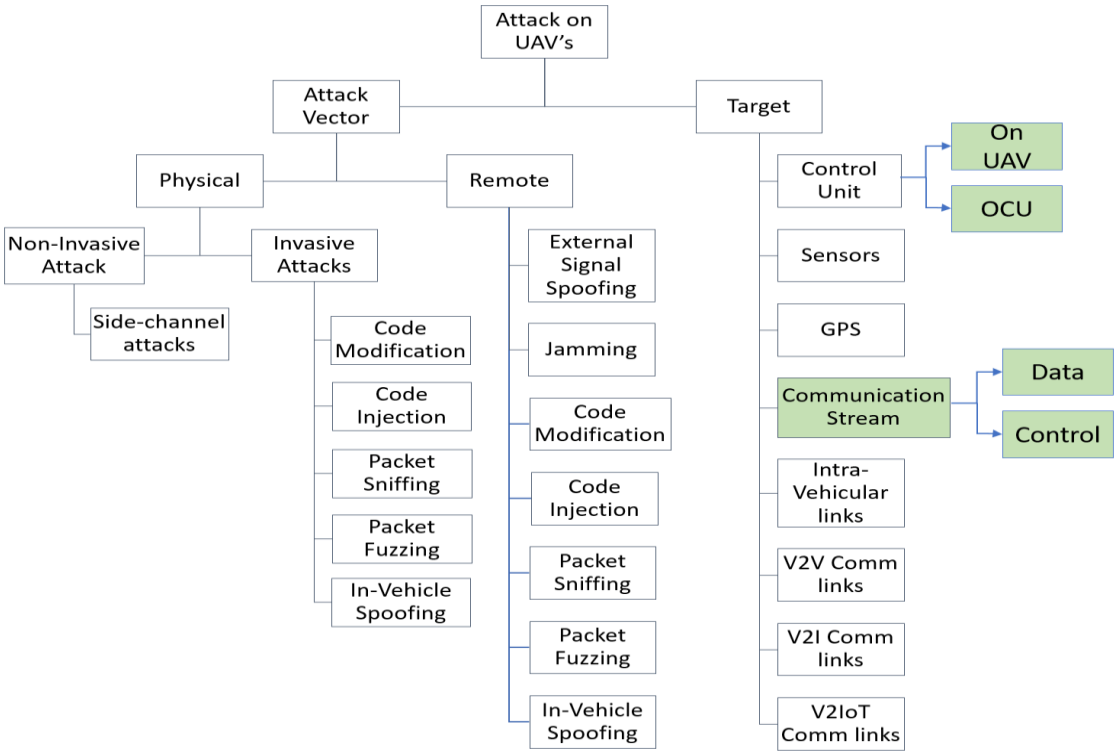

Figure 3: Attack taxonomy which includes all possible attacks with a focus on autonomous vehicle, along with an expansion (In green: details regarding vulnerabilities for UAS). In terms of categorization, is can be listed in five categories: Attacker, Attack Vector, Target, Motive, and Potential consequences [8].

Another study by Mansfield et al [9], which has a main focus the UAV used by the United States of America armed force, presents the severity of the liability issues of drones in the extremely dangerous sector of armed drones. The paper analyzes cybersecurity issues and specifically the vulnerabilities within the communication links and hardware of devices related to unmanned aircraft vehicles and army unmanned aircraft systems.

The study concludes that the USA armed forces do not have the needed risk assessment regarding their wireless networks and drones; furthermore it states that they have failed to create and establish the needed cybersecurity countermeasures. The authors continue about the severe exposure of the UAVs and their relevant critical information to high level of cybersecurity risks [9].

Though the study provides the needed countermeasures and expose the already known liabilities to a substantial degree, it mainly resolves around army usage of drones and hence does not cover in depth the risks and needs in a civilian UAS as an airport or a smart airport.

2.3 Artificial Intelligent (A.I) and Unmanned Aircraft Systems (UAS).

As the technology of unmanned aircraft vehicles progress, so do the computation capabilities which they are able to possess. Hence according to studies [11-12],[14] they can now be used for more complicated tasks such as data mining, swarm logic or even brute force enhanced with machine learning attacks.

The implementation of data mining in UAVs has been analyzed and presented in a variety of papers and books. In the paper of Hasan et al. "Swarms Intelligence and Their Applications in Data Mining" [13], is stated that UAVs with low-end capabilities can be used in order to create a swarm capable of acquiring large quantities of data. Those simple UAVs will be in a connection with a data point with the computational power to handle the information given by the swarm and store it accordingly. Creating in this manner, a huge security liability regarding the control and use of such systems, along with the proper and legitimate use of the acquired data.

A study published by Salamatian et al [10] presents the concept of brute force cyber-attacks powered by artificial intelligence algorithms. Most precisely machine learning can be used to enhance the probability of a successful brute force attack by analyzing the dictionary of passwords previously used. According to the research, the uses of such algorithms (namely Torch-rnn) increases the success rates in comparison with systems that utilize brute force attacks but not use artificial intelligence-based algorithms. The paper also analyzed the use of pattern recognition techniques as an alternative A.I algorithm for brute force attacks, producing the same results.

The U.S.A. based cybersecurity firm "Fortinet", has published a press release which evaluates the risks regarding the use of UAVs and their utilization in swarm logic in order to conduct cyber-attacks against devices connected to internet of things [11]. The above mentioned press release, with the title "Swarm Cyber attacks Target the Internet of Things (IoT) with Growing Intensity" analyzes the exploitation of systems to such attacks and states that the volume of cyber-attacks against IOT devices have quadrupled [11]. While new botnets specifically made to target IoT devices like Reaper and Hajime are now able to exploit multiple known vulnerabilities simultaneously. The study continues by predicting that those kind of complicated attacks are going to expand over the next year along with the rise of technologies like self-learning swarmbots and hivenets, while at the same time suggesting that the only defense against such cyber-attacks is an integrated

security system. Due to the limited time gap which such cyber-attacks must be met with, the systems should use self-learning techniques and algorithms in order acquire the ability to make autonomous decisions [11].

While the mentioned press release addresses the issues of swarm logic attacks, it focuses around the swarms of botnets, without assessing the use of UASs in such attacks. Those cyber-security aspects are in need of further evaluation which the current thesis will address accordingly.

2.4 Unmanned Aircraft Systems (UAS) and counter measures.

Crucial part of cybersecurity against unmanned aircraft vehicles is the counter measures which can be taken in order to deny the physical presence of them inside the premises of the critical infrastructure. A claim which, according to "Heimdal Security" [15], a company specialized in cybersecurity, is reinforced from the expectation that the anti-drone market size is predicted to reach almost 2 Billion dollars in the next 5 years.

According to the same source, this is also the reason why numerous companies or even whole countries have invested in the research and development of such equipment. Such proposed system is the "KNOX" [16], a system developed by the European Commission which aims to identify and restrain the subject UAV. Moreover, it is able to locate and identify the suspect UAV before the drone has initiated its malicious act. This is accomplished by monitoring and targeting the communication channel from which the UAV in communicating with the user. Once the frequency is detected the system is capable of isolating the signal frequency and then proceeds by jamming the signal without affecting any other wireless communication except the targeted one. Additionally, the targeted unmanned aircraft vehicle is forced to land in a predefined and controlled area for further evaluation due to the interference.

A similar patent by Steve Shattil and Robi Sen [17], has been proposed in order to counteract act malicious acts conducted by drones. More specifically, the radio signals of an area are scanned in order to monitor the various signals. Then a classifier is going to determine whether the unmanned aircraft vehicle constitutes a threat. Should the UAV be

categorized as a threat, the system exploits the communication protocol of the UAV as a countermeasure.

Based on the aforementioned, the use of physical countermeasures against unmanned aircraft vehicles must be part of this thesis in order to provide holistic and complete results. More methods regarding the issue are going to be analyzed in the following chapters of this thesis.

3 Technical analysis of UAS

This chapter will have as an initial aim the introduction of basic concepts around the technologies, evolution and capabilities of UASs. In the subsequent sub-chapter more complicated functions, concepts, liabilities and attack patterns are presented.

3.1 UAV history and evolution

While the modern conception about unmanned aircraft vehicles is fused with the technologies of the 21th century, their existence and realization was conceived as early as 1849 AD. The term Unmanned Aircraft Vehicle (UAV) itself is not standardized, but according to many sources, it is stated as a reusable autonomous aircraft-vehicle or more precisely as "a reusable aircraft that has the ability to perform a variety of missions" [22-23]. The first recorded use of UAV for scientifically purposes is credited to Douglas Archibald who in 1883 AD modified an anemometer in order to work properly once attached on the line of a kite [22]. He then used his invention in order to measure altitudes up to 400 meters and reuse it accordingly, hence categorized as a primitive form of UAV.

The term "drone" as an alternative to "UAV" was also introduced during this period of time [22][25]. Its origins are believed to be the introduction of a UAV version of "DH.82B Queen Bee". This radio-controlled aircraft developed for the British armed forces at 1936 gave the spark for a more convenient name to be used. Since the UAV was radio controlled and thus did not possess a will, it was named drone, to resemble the relative mindless drones found in bee colonies.

In 1934, the first shop dedicated on selling radio-controlled UAV meant for hobby activities was open by Reginand Denny in Los Angeles [26]. This initiative exploited the use of cheap and easy to made UAV for the purposes of amusement and its success led its owner to adopt the same idea in the military.

Many more models followed along with the introduction of new technologies like, bidirectional communication, jet engines and more sophisticated sensors, but drones usage was mostly limited to military uses [22-23], [27], [28]

The commercial, non-military use of unmanned aircraft vehicles, as we know them today will begin in the year 2006, with the commercial drone permit issues by the Federal Aviation Administration (FAA). The so called "drone-era" started with the announcement

of the founder of Amazon "Jeff Bezos", that his company was examining the concept of UAV used for deliveries and hence commercial use [29]. When this announcement was made, the general public still didn't have enough experience with the utilization of drones for such uses and considered the statement to be a product of science fiction.

Following the initiative of Amazon company, major commercial companies invested in drone research and capacities, with Intel alone spending more than $60 million in drone related projects. Moreover the publications gained from the increasingly use of drones, led to the adoption of this technology in a variety of sectors such as real estate, private security, media, agriculture, media and even mining [29].

Furthermore, new companies were created with the scope of creating new services, technologies and products centered around unmanned aircraft vehicles [30]. Companies like Autel Robotics have created a drone focused on the task of photography from aerial stand and view, while it can also be used as a mean of aerial exploration.

The technology and ambition related to drones in the current day and era, created drones that are expected to be deployed and function even in the outer space. A research project conducted by National Aeronautics and Space Administration (NASA) with the scope of propelling the space exploration, is experimenting in the creation of two rotocrafts drones in the next seven years [31]. The mentioned drone is called "Dragonfly" and its mission is to land and explore the Titan, a Saturn's moon and according to NASA the technologies involved are very mature on Earth and hence the project is by far realistic.

3.2 UAS capabilities

Since this thesis is centered around cybersecurity threats in critical commercial infrastructure posed by commercially used unmanned aircraft vehicles, this chapter will focus on the capabilities on commercially available technology and UAVs. Though cybersecurity threats can be also realized by military purpose drones, their capabilities and technologies are classified, and hence only small references will be made regarding their use. Moreover, this chapter is going to include only information regarding the range and carrying capabilities, since specifications like size, weight, sensors etc, are analyzed separately along this thesis.

Along with the evolution of the technology regarding fuel consumption over the latest years, many related concepts and practices have become available to companies developing and manufacturing commercially available UAVs [32]. And while according to the study " UAV Research and Evolution in Long Endurance Electric Powered Vehicles" [32], it is stated that there is a need for further research and development in many related fields like performance, cost, power storage, avionics etc., their abilities as presented below are rather spectacular.

They are three main technologies used as power supply that are affecting endurance and provide long flying time, based on the type of batteries and even charging times. Most precisely, according to a press-release by Luke Dormehl [33], they can be distinguished as UAVs using batteries, hybrid UAVs and internal combustion engine UAVs.

1. Flying battery drones as they are called, models like "US-1", can stay in air for more than 2 hours at a time [34]. This is achieved by a large lithium battery pack which also comprises the majority of the weight of the UAV. The US-1 is a commercially available quadcopter, weighting 15.7 pounds with a frame of 66cm and top speed of 70km per hour. Even more worth mentioning is the fact that along with a variety of sensors such optical and thermal, it also processes the ability to carry a payload of almost 2kg and stay on air with it for 78 minutes.

2. Hybrid power drones utilize a technology which incorporates both an internal combustion engine and an electric motor [35]. The engine is used to power an electrical generator which in turn drives the motors of the UAV. Models like "Hybrix.20", claim to be able to achieve up to four 4 hours of hovering without the need of refueling. At the same time it can sustain a payload of 2.5kg for 2 hours and at a cruising speed of 50km per hour [36].

3. Internal combustion drones are incorporating a internal combustion engine to directly drive the propellers used for achieving hovering [33]. Models like the "Yeair" can carry an incredible payload of 6kg and stay on air for an hour before the need of refueling [36]. Moreover, they are models centered around power consumption and not payload capacity like the model "VA001" [33], which has the record for the longest internal combustion-powered flight (five days and one hour).

3.3 UAS cybersecurity liabilities

Another crucial aspect of cybersecurity and UAS is the possibility of a malicious cyber-attack conducted against the unmanned aircraft vehicle itself. This statement is strongly supported [2] by experts in the field of cybersecurity and it is scrutinized analyzes accordingly. As explained in the "State of the art" chapter regarding the security liabilities of UAV, each main category is going to be presented in the following pages.

3.3.1 UAV and spoofing based attacks

As explained by the paper "Effect of Spoofing on Unmanned Aerial Vehicle using Counterfeited GPS Signal" [38], those attacks target a very crucial function of the UAV, which is the true knowledge of geographical positioning. This attack is based on the fact that non-commercially available drones, do not receive an encoded GPS signal. This kind of attacks are not feasible to military drones due to the use of encoded GPS signals and thus the information contained cannot be altered [38].

Attacks like the aforementioned ones, start with a signal that imitates the GPS signal that the drone uses for navigation and, as explained the same paper, the attacker is able to first confuse the drone and draw it a halt. Given enough time and proper equipment, the attacker is then able to guide the UAV in a specific location by adjusting the fake GPS signal emitted.

Another kind of spoofing attack initiates with proper monitoring of the telecommunication link between the drone and the controller. By monitoring this link the hacker is able to acquire the vital communication information like the MAC addresses used and then imitate the signal of the controller itself, thus jamming the drone to a halt or even guiding it to a specific location [39]. Such attacks under proper circumstances can even lead to complete control over the drone.

3.3.2 UAV and control communication stream attacks.

These kind of attacks have as a target the failure of the communication-control between the controller and the unmanned aircraft vehicle and hence the loss of control over the drone. As it is explained in the paper of Rani Et al "Defense Techniques Against Cyber Attacks on Unmanned Aerial Vehicles", such malicious acts have as target the halting of operations and movement executed by the UAV [38]. The study explains that those attacks are conducted by monitoring and targeting

the wireless communication. With the acquisition of client related identification, the attacker floods the drone's access point with communication requests and forces it to use all its available memory. This intervention leads to less availability to perform requests and results to denial of service "DOS" or de-authentication from the UAV access point.

In other words, the goal is to make the drone unusable or even force it land, rather than taking control of it or stealing data. Hence it is a common method/attack used by the law enforcement against a suspect drone without damaging the drone or endangering personal information [39].

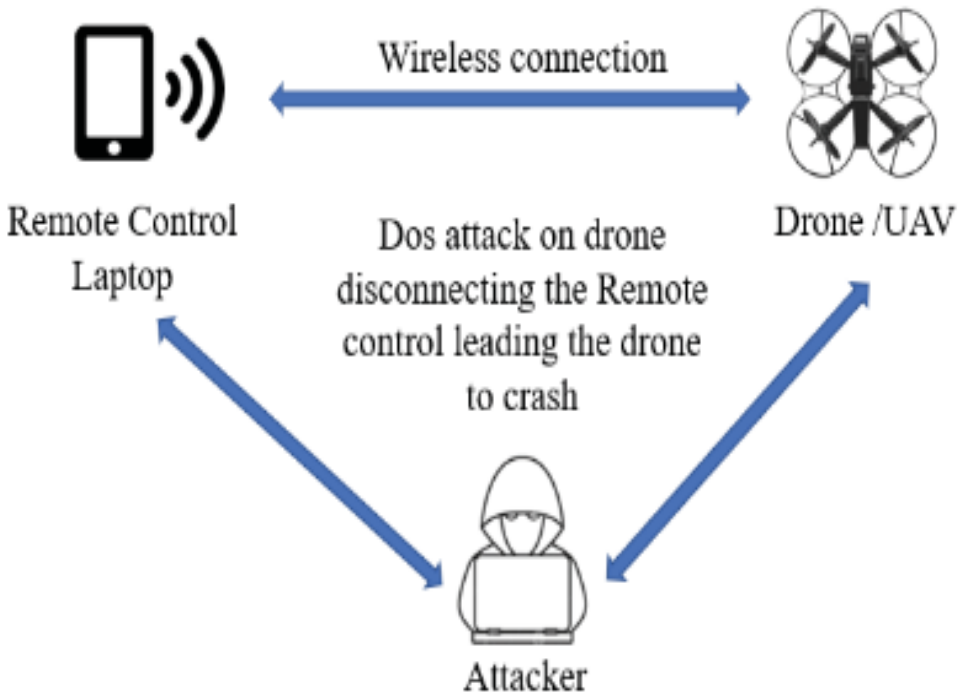

Figure 4: Illustration of and attack at the control communication stream [https://csce.ucmss.com/cr/books/2018/LFS/CSREA2018/ESC4302.pdf]

3.3.3 UAV and data communication stream attacks

The "data communication stream attacks" have as goal the extraction of the data communicating from the unmanned aircraft vehicle towards the controller without the intention of taking over the drone or jamming it itself [38]. Subsequently the attacker aims to steal information while keeping its action unknown to the user.

The above type of attack is achieved through the use of packet sniffing and packet capturing methods. It is based on the exploitation of nonexistent or simple-standardized encoding of packets which can found in the communication protocols of commercially available drones [39]. Hence it is an attack type that has as a main target the commercial drones and does not affect the military purpose ones due to the already explained reasons [38].

By utilizing the above techniques for malicious acts the attacker is able to steal information like live-video capturing, position of the drone and of the controller, measurements from the sensors or even extraction of information already stored in the unmanned aircraft vehicle [39].

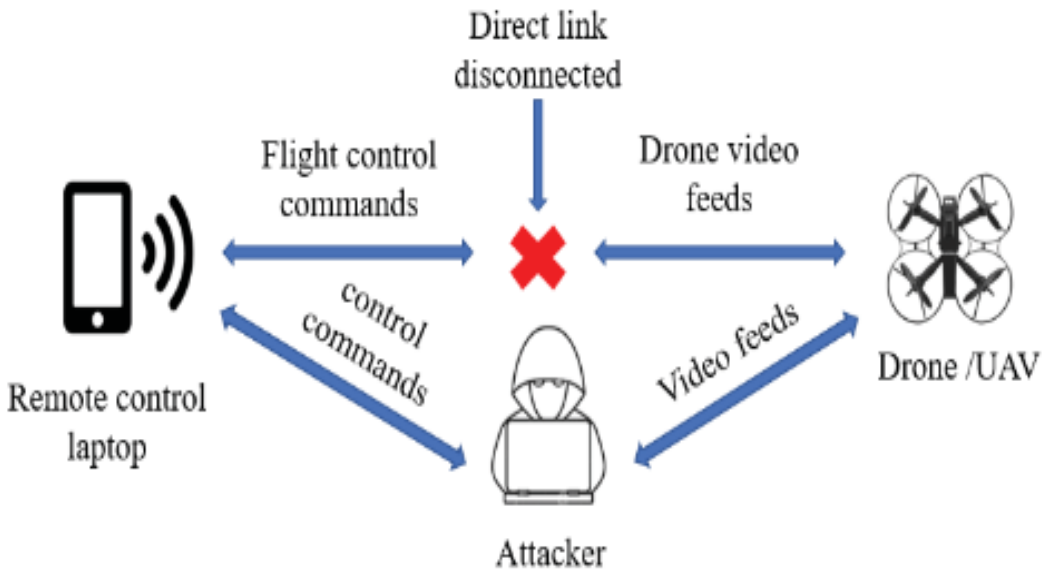

Figure 5: Illustration of and attack at the data communication stream [https://csce.ucmss.com/cr/books/2018/LFS/CSREA2018/ESC4302.pdf]

4 UAS and espionage

In this chapter the abilities of UAS to act as means of espionage is going to be presented. Additionally a number o cases related to UAS and espionage are going to be analyzed both from technical and simplicity point of view.

4.1 UAS and espionage

The most important factor to consider when studying the threats posed by UAS in regards of espionage, is that the number of commercial UAS available publicly is very large, and continues to grow each year, meaning that there are a lot of vehicles that can be used with malevolent intent. The FAA (Federal Aviation Administration) is the infrastructure that is responsible for UAS handling and control in the US. FAA notes in its 2018 forecast report that the commercial UAS numbers are growing exponentially, and more than 7 million vehicles are predicted to be sold by 2020 [106], while at the same time the regulations regarding commercial UAS usage remains inconsistent and irregular [106]. This lack of control renders the UAS an aspiring platform for malicious use, due to the very nature of such a machine that is versatile and loaded with a multitude of sensors, including audio and visual recording.

During the recent years, a variety of incidents regarding UAS usage for espionage purposes have occurred. This has led the scientific community to create case-studies and make assumptions for the implication in cybersecurity which the rapid expansion of commercial UAS number creates.

4.2 Using commercial drones for espionage

DJI (Da Jiang Innovations) is a Chinese company that specializes in producing commercial UAS (mostly referred to as drones), targeting civilian and industrial use. On 2017 and while a lot of large scale companies across the US were using DJI drones, the US army issued a note prohibiting the use of DJI drones for military purposes. Although no official reasoning was given then, shortly after a bulletin report from the SIP

department of Los Angeles became public, warning the civilian users of DJI drones that DJI is likely disclosing sensitive data to the Chinese government, and is using these data to conduct espionage on US industries [107].

The bulletin calls on an article of the New York Times [108] that studies the same subject, and starts its assumption by analyzing the terms of agreement of the DJI software that accompanies their aircraft systems. The terms contain a worrying sentence, warning the user that "your flight data might be monitored and provided to the government authorities according to local regulatory laws" [108]. Furthermore, the same article invokes an interview of a DJI representative, who during a briefing session with Chinese government representatives, he ensures them that the company complies with the request of the government to hand over data that was gathered by the use of their drones in foreign countries.

The report concludes by stating "with high confidence" that DJI is specifically targeting the US market in order to obtain information and footage regarding critical information of US utilities, such as water storage infrastructures and railroad systems.

This incident signified the dangers of the increasing popularity of commercial UAS. These drones have the means to monitor and store a variety of data, from coordinates and flight routes to video footage. Depending on the software of the system, a manufacturing company like DJI may access utilize, or event takes advantage of this information. While this specific incident is rooted to the political and marketing relationships of China and the USA, it creates a precedent of general information leaking for espionage activities. Since such sensitive data can be gathered by the manufacturer, it creates the need to control the software that each company uses, and whether each manufacturer's system complies with the directives regarding the handling of private data of individuals.

While the DJI incident exposed to the public the dangers behind the rising use of commercial UAS, the scientific community associated with cybersecurity had already reasons to be concerned for the security risks that the drones can inflict. In 2011, and during the BlackHat annual conference two security consultants, Mike Tassey and Richard Perkins presented a makeshift UAS, based on a deprecated army model, that was equipped with specialized hardware to impersonate a GSM network and steal calls and communication. The WASP, as it was named (Wireless Aerial Surveillance Platform) was

able to fly overhead and sniff Wi-Fi networks, intercept cell phone calls of individuals, or launch denial-of-service attacks with jamming signals [109].

Figure 6: The WASP prototype in Tassey's garage [https://www.geek.com/geek-pick/wasp-the-linux-powered-flying-spy-drone-that-cracks-wi-fi-gsm-netwokrs-1407741/]

This presentation successfully underlined to major risks that were imposed: Firstly, the modifications needed for the creation of such a system are off-the-shelf products that are readily available to the retail market [110]. As one of the creators underlined, a simple 300$ drone can be used for the WASP, with only the addition of a lightweight Linux computer, two Wi-Fi cards, an IMSI catcher and an antenna to spoof a GSM cell tower and intercept calls. These modules can be easily bought from stores associated with electronics and prototyping. The second risk is that the assembly is relatively simple, and most IT professionals associated with networking would manage to successfully replicate a WASP. As the creators characteristically noted: "You don't need a PhD from MIT to do this". [110]

The aforementioned statements underline a specific danger: that any professional individual (or an individual with an interest in such technology) has access to the materials and the technique to recreate the WASP, even at his home garage. This means

that the possibility of spying data and calls is not limited with the need of an expertise of a large company, such as the previous example of DJI, but can also be extended to civilians using modified UAS to spy on other individuals. The increasing number of commercial drones adds up to that danger, since identification of a modified one can be challenging, and the fact that drones have become a common occurrence and a usual sight for civilians, renders the public less suspicious and more prone to be spied upon.

4.3 Industrial espionage

A large part of attempts of using UAS for espionage is not targeted towards civilians, but companies and industries. In the prior incident with DJI, the bulletin published reported that DJI targeted specific companies associated with vineyards and plots of land in a specific area of the US. Some time after, the owners of many of land plots, were approached with buy offers by chinese companies [107]. The US intelligence claims that the chinese used footage from the DJI drones to calculate the potential value of each vineyard and plan their purchases accordingly. This event signified the usability of UAS as a surveying mechanism, and that drones can be used to scout a region for potential buyers, for example giving information about specific cultivation areas, or details regarding a plot of land. This capability can also be extended to anything related to real estate, since a UAS can survey a whole neighborhood for an extended period of time, providing information regarding traffic hours, night life, and other factors that may influence the value of a land plot. But land survey is not the only concern for the industries that is carried by UAS.

Unmanned aircraft systems or drones can easily bypass physical security measures leaving companies vulnerable to attacks. In 2016, a commercial UAS crashed into the new Apple building, although special measures have been taken for the campus to be considered a “no drone zone” [110]. Tesla and Facebook campuses have suffered similar events. These incidents signify the ease with a UAS can invade an otherwise secure and guarded private property of a company, due to its small size and versatile movement. Manual monitoring of the air zone around a building is not always easy, especially for newer, small-scale drone models. Once the UAS is inside, it can perform a variety of intelligence breaches, from simple video monitoring, like the example with the DJI, to

Wi-Fi network sniffing, as it was the case with the WASP, or perform other, more dangerous functions.

In 2016, scientists of the Ben Gurion University in Israel released a paper that combined a previous project of them with the espionage capabilities of a UAS [112]. The team had previously created a malware that upon injected into the computer through USB, it would code the data inside the hard disk through and algorithm that resulted in blinking the driver LED light in a specific way, in order to pass along the data inside. A small drone stationed outside would fly to a nearby window in order to be able to pinpoint the LED blinking, and it would receive the light messages, decode them, and send them to the intended recipient. This method successfully managed to snitch data from "air-gapped" systems, systems that are isolated from the internet, and thus considered safe from most hacking attempts.

Figure 7: footage from the video presentation of LED-it-Go paper depicting the drone's POV while recording the signals. The tiny light source indicated is the hard disk's LED [https://www.youtube.com/watch?v=4vIu8ld68fc]

The results of the experiment, that combined highly sophisticated malware and UAS espionage capability, was to successfully hijak information that would be impossible to be accessed before, and this proved how much the UAS have changed the cybersecurity dangers that an industry used to face until now

The aforementioned incidents create a clear picture of the various espionage methodologies that can be implemented or enhanced through the use of drones, and are but an indicator of the variety of ways a UAS can be used for spying on individuals or industries.

5 UAS as a mean of mapping and the use of RFID sensors.

This chapter is going to present the evolution and use of RFID technologies in UAV, moreover related algorithms which are used in localization and mapping are going to be analyzes. Last but not least the connection and usage of the two technologies is going to be explored and presented.

5.1 RFID technology and UAV

The idea of using Radio Frequency Identification (RFID) technology in order to track down and localize its position has been used extensively both in industry and academia, while a research conducted by IDTechEx forecast that modules which utilize this technology like RFID labels, tags etc. will grow to a market with value over $13.2 billion by 2020 [40].

The RFID technology as we know it in this time and era was introduced by Steven Depp, Alfred Koelle, and Robert Frayman in 1973, though the idea and first attempts go as back as 1948 (Harry Stockman) [41]. The principles on which the technology is based are the electromagnetic fields and can be categorized based on the role which they are designed to accommodate or based on the present or absent of power supply which they need in order to function [42].

Based on the role they can be distinguished as “readers” or as “tags”, with the later one be able to further categorize as “active” or “passive”. Active tags operate with the use of small power source, usually a battery which provides them with the necessary electrical power I order for their circuit to create the needed radio waves which the reader is going to receive and use to truck the RFID rag. This kind of RFID tags have the advantage that they can be trucked form distance, usually a few hundred meters, but they possess the disadvantage of limited life-spam due to the nature of their integrated battery [42].

The passive RFID tags collect the necessary electric power from the signal produced form the reader radio waves. By utilizing the magnetic induction principal of Faraday, the signal of the reader creates a larger alternating current in the antenna of the tag, which in turn creates and alternating magnetic filer in the coil of tag. Resulting to production of electric energy from the coil which is used as power source in order for the tag to

propagate radio waves from its antenna. Those kinds of tags should be located near the source of the radio waves produced by the reader in order to function, but their lifetime can be stated as "indefinite", while simultaneously their size is much smaller than the active tags, since they do not require a component like a battery [42].

The utilization of the above technology and equipment in unmanned aircraft vehicle is presented in two forms: self-localization of the drone itself or for localization of RFID tags in the operational environment of the drone. More precisely research papers like "Drones relay RFID signals for inventory control." have developed a system which incorporates drones equipped with RFID readers for the purpose of inventory management. The drones are used in order to scan, identify, track and relay back the RFID tags that have been scanned in an area like a warehouse or a parking for cars etc [45].

Moreover, research papers like "Localization of RFID tags for environmental monitoring using UAV" [44], are analyzing the functionality of such innovative ideas. The mentioned paper centers on the implementation of a method to localize and track tags which have been preset in an outdoor environment. The unmanned aircraft vehicle scans the area with the use of an RFID reader and based on its geographical position and measurements on the strength of the received signal, it is able to locate the geographical position of each tag. Providing in this manner a map which contains the coordinates of each and every tag which has been able to scan and localize.

In addition, RFID that are currently available in the market include the ability of both read and write in their memory. Though the memory of such writable memory RFID are in the size of a few thousands of bits, their abilities and memory volume is expected to grow even more, according to the paper of Roy Want [42]. Hence, introducing a variety of new procedure able to be covered by drones equipped with RFID readers.

5.2 S.L.A.M

Simultaneous Localization And Mapping (SLAM), resolves the issue of a robot constructing a map of an area or environment based on topological measurement or calculation of the geographical position of the features which resides insight the mentioned area [48]. The robot, or in our case, the unmanned aircraft vehicle initiates its

service without the knowledge of both the environment in which it must function nor its own position in contrast to the environment itself. The UAV is called to position itself in the map which creates while in the process of still creating the map itself hence giving it the name S.L.A.M. A variety of algorithms, techniques, implantations and usages have been created in order to address and utilize such a concept.

The first successful implementations of SLAM were mathematical models which they are based in sensor fusion and posterior probabilities of the point of interest in the map. Techniques like “Kalman filter” and “Particle filter”, also known as Monte Carlo methods, are examples which incorporate the above models. Worth mentioning is the fact that Kalman filter, was so robust and accurate, that show extensive use in the aerospace engineer, while it was part of the algorithms that guided the Apollo 11 lunar module to the moon and back [46]. Moreover its success and simplicity paved the way for the adaptation of this model, as base for a variety of SLAM techniques like “Extended Kalman filter, “Hybrid Kalman filter”.

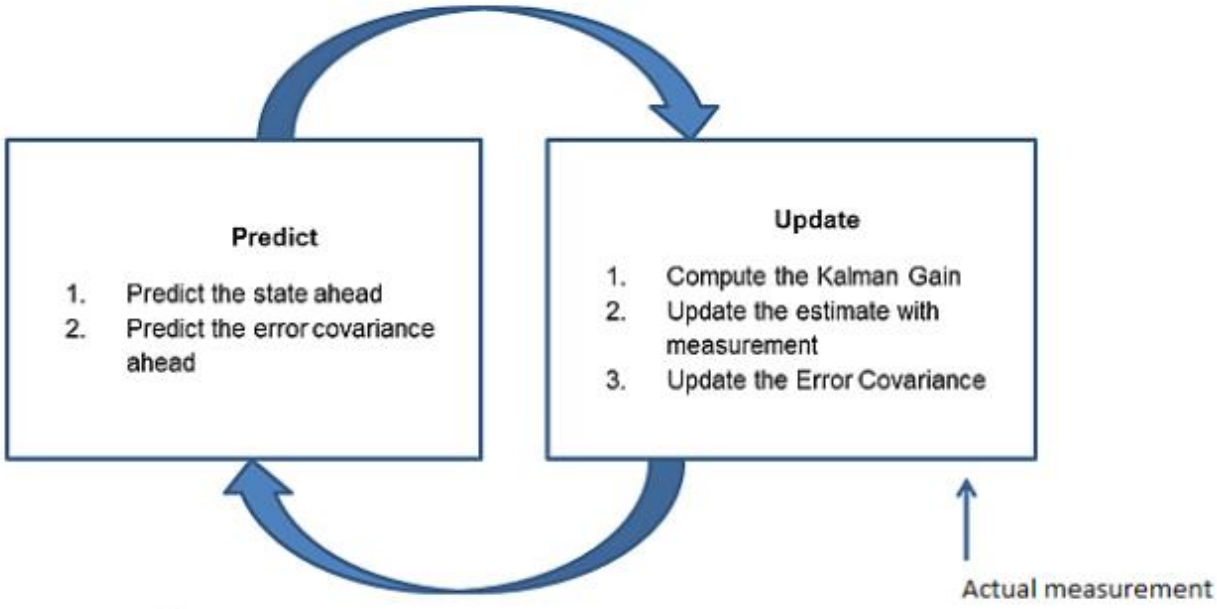

Figure 8: A depictions of steps which the Kalman filter (SLAM) can be distinguished [https://towardsdatascience.com/an-intro-to-kalman-filters-for-autonomous-vehicles-f43dd2e2004b]

Since the ability of a robot to be able to localize itself in an environment while simultaneously be in a position to measure the environment and produce a map of it, it is considered a vital prerequisite to be called “complete autonomous”, it has paved the way for further improvement which utilize all the sensors and capabilities of a robot or drone [47].

Algorithms like “FastSLAM are able to process and calculate large volumes o landmarks without the computational needs of techniques like regular Kalman filter. The term “Landmark” is used to describe a point of interest in the map and more precisely its geographical coordinates based on the map provided by the SLAM technique. A “landmark” can be the position of an object or an RFID tag which the reader of robot can capture. While last but not least, the landmark in SLAM, is used both for the localization of the robot itself and for acquisition of the information regarding the accurate position of the landmark itself [1].

As it is mentioned in the paper “FastSLAM: A Factored Solution to the Simultaneous Localization and Mapping Problem” [48], Kalman filter based techniques require quadratic time to in-corporate each sensor observation in the number of each and every landmark. According to the same paper, the FastSLAM algorithm was able to handle more than 50.000 different landmarks, which as it mentioned, it is a volume far beyond the capability which can be achieved with the older approaches.

.

5.2.1 SLAM and UAVs

As it was explained and stated in the new chapter, an autonomous vehicle must be able to execute SLAM and SLAM based procedures [48]. This in term led to the introduction of such techniques and models to unmanned aircraft vehicles. As it is going to be presented in the following chapters, this utilization has created many opportunities in combination with the aviation and hovering ability of a drone.

In the paper of Bryson et al “Building a Robust Implementation of Bearing-only Inertial SLAM for a UAV” [49], the idea of an implementation of SLAM algorithm able to function over a UAV is presented. The algorithm utilizes bearing-only observations while the features or landmark are extracted from the environment with the deployment of a single color vision camera [49].

Going a step farther the research paper "Multi-UAV collaborative monocular SLAM" presents the utilization of multiple drones called agents in order to handle the task of SLAM. [50] The same paper states that multiple tasks can be achieved with the integration of many UAV in a collaborate grid rather the use of a single one. Although the described implementation requires the use of a central server which is unburden with the task of handling the information produced from the agents, it also presents a new era of information that can be extracted. Paving the way for a plethora of advantage that can be gained from SLAM.

Moreover, it has to be pointed out, that the SLAM integration in UAV is not subject solely researched or implemented by academia and researchers. A statement which is based on the fact that companies like "Ascending Technologies" (a part of INTEL corporation) is offering UAV models and related software which are able to perform SLAM techniques along with 3-D scan of the area scanned by the UAV [51]. The Cybersecurity liabilities which such technology creates in going to be presented in the following chapter.

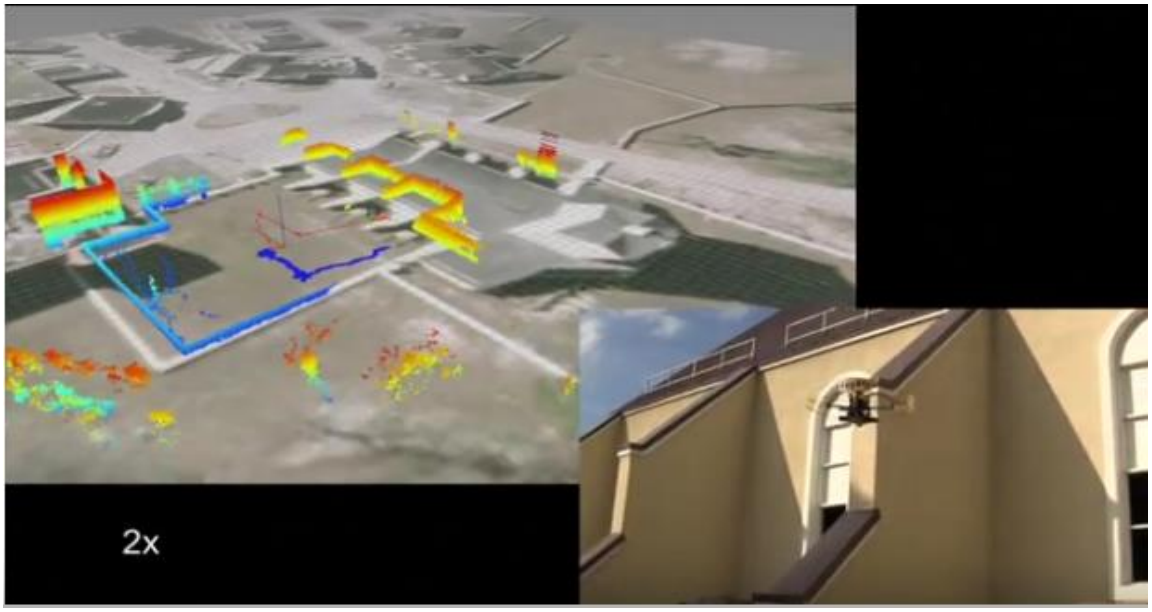

Figure 9 : An example of 3D map results, based on SLAM algorithm technique in UAV [http://www.asctec.de/en/uav-uas-drone-applications/uav-slam-simultaneous-localization-mapping/]

5.3 3D maps and espionage with the use of UASs.

Unmanned autonomous vehicles offer a variety of options which they can be used for malicious acts and most precisely, espionage. Moreover the user/controller of the drones, can be located in a safe and distant position, giving him the opportunity to avoid capture in the event of a failed attempt. While at the same time the drones are capable of receiving high definition resolution images or live video stream to the controller even if they are located at great distances. Moreover, the video stream can be encrypted, giving drone's user another security measure in order to avoid the detection of his/her premises [52].

In addition to the mentioned information, in our time and era, a GPS device can be easily found in most UAVs. The dramatic improvement that a GPS can have in mapping and specifically in 3-D mapping is presented in the paper of Nagai et al "UAV-Borne 3-D Mapping System by Multisensor Integration" [53]. In this study, a mapping system based on an unmanned autonomous vehicle, able to produce detailed 3D map is presented. The system has the advantage that it can be achieved with low-end equipment and without the need of decreasing the detail that the map can incorporate. Hence this specific UAS can be assemblies by cheap parts available to the commercial market.

While this paper aims to be utilized at disaster sites, it proves that it is possible to achieve 3D [53] detailed mapping with the need of expensive or military restricted equipment and hence similar technology which utilize the same advantage can be used for malicious acts as espionage.

In parallel, RFID technology as it was introduced to the relative chapter, has enabled the creation of a variety of RFID tags in all shapes and sizes [42]. RFID with the size of rice grain are now commercially available and hence their trucking can be a hard task especially in the case of passive RFID tags. Those tags (as explained in the previous chapter) only emit signal if the located insight the range of a specific frequency pre-defined signal.

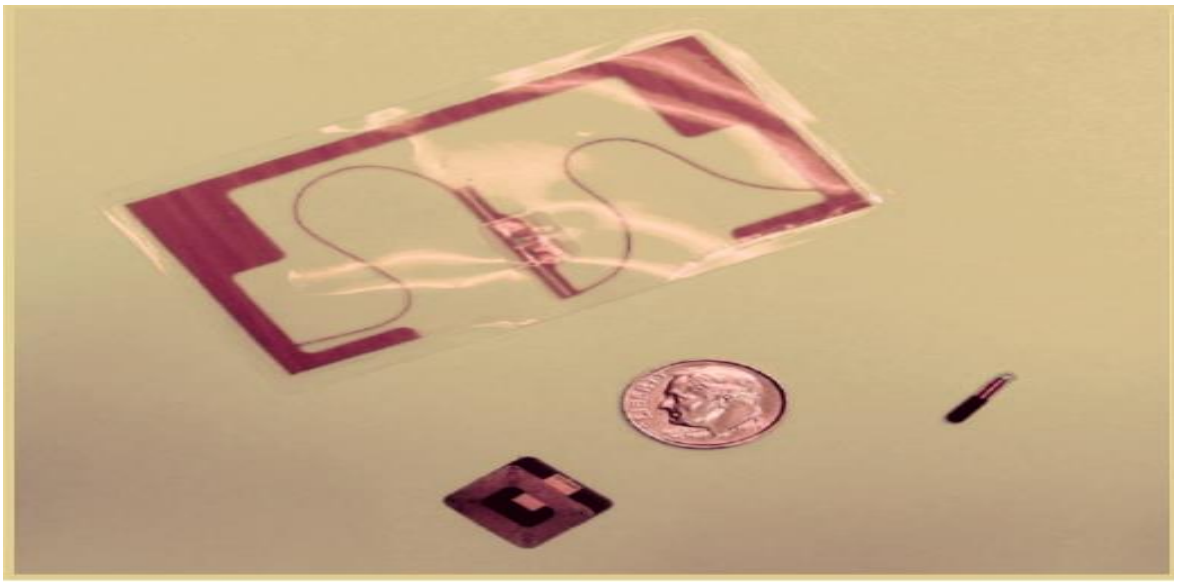

Figure 10 : Passive RFID tags side to side by a penny in order to demonstrate their small size [42]

Based on the aforementioned, this paper proposes the conception of a cyber-attack which utilizes the RFID and 3D-mapping technologies in order to create a tagged and mapped version of the critical infrastructure.

More precisely the already available and proved technology of 3D-mapping with the aid of GPS can be used in order to map the critical infrastructure. This information is created with the use of a SLAM method which can be greatly improve in terms of accuracy with introduction of RFID tags in the environment distributed by the drone itself [54]. As presented in the paper "RFID Technology-based Exploration and SLAM for Search And Rescue" [54], this implementation also improves the coordination of multiple drone simultaneous, a concept which this thesis is going to present in another chapter.

Last but not least, we propose that the RFID tags themselves, can be used in order to specify with great accuracy specific weak points in the under cyber-attack infrastructure, those are going to be act as point of interests or even directly targets in the further exploitation of the obtained 3D-map. Providing in this manner an extra critical information and at the same time improving the accuracy and value of the information.

6 UAS as a mean of Wi-Fi network mapping

In this chapter the functions, mechanism and liabilities of Wi-Fi networks are been presented, along with types of cyber-attacks and their outcome. Followed by the proven capabilities which drones posses and which the can be used in order to target a Wi-Fi network.

6.1 Network mapping and security liabilities

Wireless networks such as those created by regular Wi-Fi routers in our houses, can be found everywhere and their range of usage extends from internet access point in homes and offices to whole corporate data centers. Their intent (in most of the times) is to provide cable-free connectivity and hence avoid the related visual and practical problems which arise when they used in great numbers or lengths. Their use has changed the modern society and continues to shape it with each new network function, but according to many experts the danger those networks possess is seem-less as the network itself [55] [56].

A wireless network aims to establish a communication link between two or more devices, this communication link it is achieved with the use of radio transmitting protocol such as the “IEEE 802.11” and aims to create a point to point wireless communication. The same protocol states that communication link must be able to handle signal fading due to distance and physical obstacles and achieve resistance to factors that produce of signal jamming [55].

The network it is consisted by an access point such as a Wi-Fi router, many times referred to as hot-spot or even beacon and one or a number of wireless nodes that are the end-part of the network such as a cell phone device. The access point transmits a radio signal containing the needed information for a device to connect to the wireless network, with the most important of those to be the service set identifier (SSID). The node detects that signal and after decrypting the information contained, it attempts to connect to the access point providing the credential given by the user.

The access point has the ability to support multiple nodes simultaneous and hence the need for an authentication layer to be present before the connection is allowed. Hence it is in the jurisdiction and responsibility of the access point to provide a secure connection by utilizing the mentioned technique before enabling the date transfer towards the node to

take place. It is also designated with the task of monitoring the packet transmission and data integrity during the radio transmission of the communication [55].

Due to the nature of wireless network, the wireless communication that takes place can be easily captured and or even replicate. The same issue is not present in wired networks since the signal is transmitted through physical cables and hence the signal is not freely transmitted in the air. Although the signal transmitted by a wireless network is encrypted for this specific issue, the functions that produce this secure radio channels are not perfect.

More precisely, the more common practice in order for the network to create a secure connection is the establishment and utilization of the pre-shared authentication key. Also known as SSID authentication, in this security protocol, the client sends an authentication request which is encrypted based on the key (private, public or both). The access point decrypts the message request based on its own predefined key, hence a successful decryption will suffice in order for the client to be accepted. Should the massage not be able to be decrypted based on the access point key, the authentication request is dropped from the access point.

The wireless network attacks can be categorized into two main categories, the active attacks and the passive attacks [57]. This classification is based on the target that the attack aims, the passive attacks do not aim the network and its services, but aim to obtain the data transferring through the network. In other words, they do not interrupt the communication stream nor affect the data. The active attacks have as a target the disruption of the communication services and functionality of the wireless network. This also includes the fabrication or alteration of data transferred through the network. In the following line, the most frequently used of active and passive attacks are presented:

1. Man In The Middle Attacks (active attack): Also known as “replay attack”, aims into tricking clients to connect on an rogue access point that impersonates the original access point. This is achieved through the creation of a fake wireless signal with substantial signal power over the original one [57].

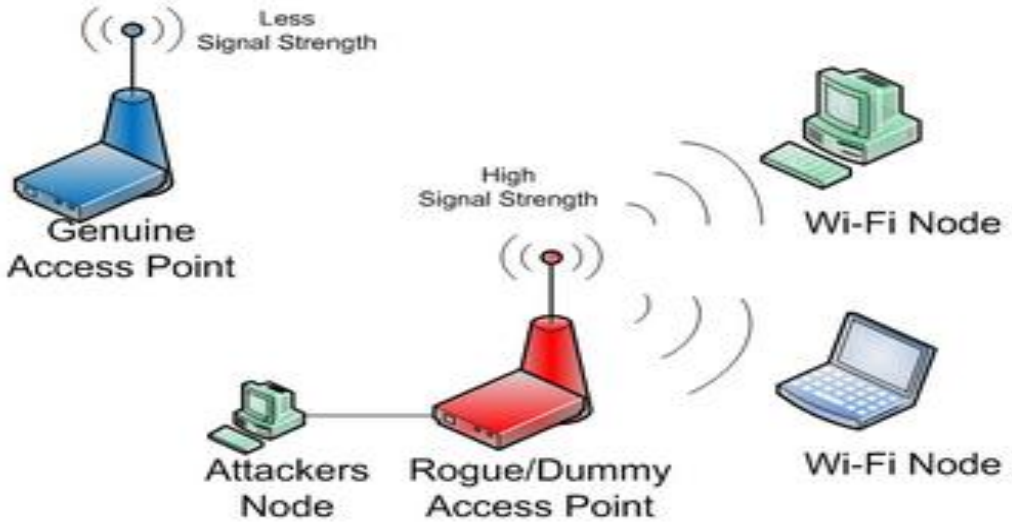

Figure 11: An illustration of “Man in the middle attack” and the mechanism which it is based on [2]

2. Wireless network signal jamming (active attack): Those kind of attacks take advantage the mean through which the data itself is transmitted. It targets the RF spectrum which the access point uses to send and receive radio signals through the use of a powerful antenna. The antenna emits RF signals powerful enough to overwhelm and disrupt the signal send from the access point or which the access point meant to receive. This has an outcome the jamming of the communication channel itself due to the RF noise and pulse emitted, holding the wireless network to a stop [55], [57]. Such attacks can take place from geographical location remote to the targeted access point, while a closer proximity can make the results of the attack even more effective.

3. Denial Of Service attacks (active attack): Most commonly known as “DoS” attacks, aim to make a computer service unavailable to its meant user or users. There is a plethora of different implementations that can achieve such a result, mostly depending of the category of the service targeted. While they can be categorized

into two big groups, the “flooding attacks” and the “crashing attacks”. The flooding attack, consist the most simple and commonly used attack, and though it can be categorized even further, the main aspect remain the same. The attacker “floods” the access point with a large volume of packet requests. On the contrary the “crash attacks” target flaws or bugs in the services in order to make it unavailable/crash [57-58].

4. Traffic analysis and monitor (passive attack): Those kind of attacks do not interfere with the proper function of both the access point and the wireless communication. On the contrary, a receiver is used in order to monitor and intercept packages and information that are sent through the air. The attacker is then able to acquire information like radio bandwidth and signal strength which can help in an eminent “Man in The Middle Attack”. Furthermore, by analyzing and decrypting the packets, it is able to even acquire information like SSID, MAC address, IPs or even pattern recognition as it is going to be examined in the related chapter [55], [57].

5. Wireless network data injection (active attack): In order for this type of attack to take place, a traffic analysis attack should have already acquired the data traffic and related information. By utilizing that information, the attacker sends wireless signals containing its own packets in an attempt to trick the access point into accepting those packets over or along the original ones. In this manner, the attacker is able to alternate stored data, upload a virus, create a liability in the cybersecurity defense or even make data completely inaccessible [55], [57].

6. SSID/Key cracking (active attacks): As the name suggesting, those kind of attacks aim to break the key encoding and thus receive unrestricted access to the wireless network. Through the use of passive data sniffing and analysis over a period of time, the attacker is able to crack the key through the use of brute force over the captured data. The article “Cyber Attacks Wireless Attacks” [1], mentions that a simple number of “40.000”captured data packets is sufficient in order for the key to be exposed/crack over the duration of a few minutes [55], [57].

7. Eavesdropping (passive attack): This rather simple attack, it is also based on a previous cyber-attack that has exposed the encryption/key of the wireless network.

Hence the attacker is able to decrypt and capture all the data transferred through the cracked wireless network, without leaving any traces [55], [57].

6.2 Network mapping and UAV

As it has already disgusted in the chapter “State of the art”, drones equipped with a simple wireless antenna and software that take advantage of the access point communication software are able to sniff and capture the packages send between Wi-Fi connected devices. More precisely, papers like the “Digital Terrestrial Tracking” [5], prove that drone can be used in order to monitor an access point and capture the communication packets accordingly.

That information is then able to be used as a part of a passive attack which will gather the necessary information or the information needed in order for an active attack to take place. In the previous chapter, the connection of the passive and active attack has already been establish and proved accordingly. While the paper presented by Black Hat, paved the way with a drone named “snooby” which was able to accomplish the aforementioned, as already explained in the state-of-the-art chapter.

Figure 12: The snooby drone components (left), the snooby drone (right). It is clear from the photograph that drone consists of simple and relative cheap components [6]

In addition to the above-mentioned, an article published by "Dedrone" with the name "Cybersecurity White Paper", is mentioning that there is an increasing amount of risk possessed by UAV in the field of cybersecurity. According to the article "Snoop" attacks or infiltrate network attacks can be easily be carried out from a drone. Such attack can be carried out by a simple drone caring a "Rasperry Pi" device or even a simple transceiver in order to relay the captured data [59].

A similar article, published by Brian Buntz, depicts the threats that drones possess for cybersecurity [60]. The article present a plethora of attack types, including an incident on which an aged drone was found on the top of a company building. The drone was equipped with a second battery in order to provide power solely to the Wi-Fi antenna and related equipment. This enabled the drone to transmit packets and network related information such the position of the access point, the mentioned data if put together are composing a drone which among other s had the ability to map the wireless network.

6.3 UAV and cyber-attacks at Wi-Fi networks

As it was analyzed, every active attack requires or has better chances of success if it is provided with information which can be gained from a passive attack. More precisely the following three sub-scenarios can be accomplished as a part of a more sophisticated attack.

1. **SLAM based scenario:** A UAV able to perform 3D mapping arrives at the critical infrastructure and implements a detailed map of the critical infrastructure through the use of one of the mentioned and explained SLAM techniques in the related chapter. This UAV can also be in a position to provide a 3D-map of the surrounding area by using the technologies as the ones presented in the paper "UAV-Borne 3-D Mapping System by Multisensor Integration" [53].

2. **RFID based scenario:** The unmanned aerial vehicle can utilize RFID technology in order to create the map which is described at the previous scenario. The use of RFID tags in combination with the standard GPS method will greatly improve its accuracy. This can be achieved with known techniques like the "RFID Technology-based Exploration and SLAM for Search And Rescue" [54], which introduces the concept of the drone itself being in a position to spread out the RFID beacons,

hence paving the way for a more accurate map or even utilization of them as reference point for further exploitation.

3. **Insider threat based technique**: An insider threat can take advantage of his free entrance on the rooftop of the building and/or nearby facilities and infrastructures, in order to distribute RFID tags and mark sensitive locations e.g. operations server room, wireless routers, an array of integrated smart sensors or security cameras network. Those RFID beacons will be utilized in a future attack.

After the realization of one of the above scenarios, a UAV can initiate its cyber-attack based on the existence of the accurate map or based on pre-installed RFID beacons. The malicious drone may use that topological information in order to commence a passive attack which aims to map the network along with the positions of the access points. As it was explained, traffic analysis and monitoring can then take place in order to acquire knowledge which will be used to a following active attack or solely with the intention of stealing data.

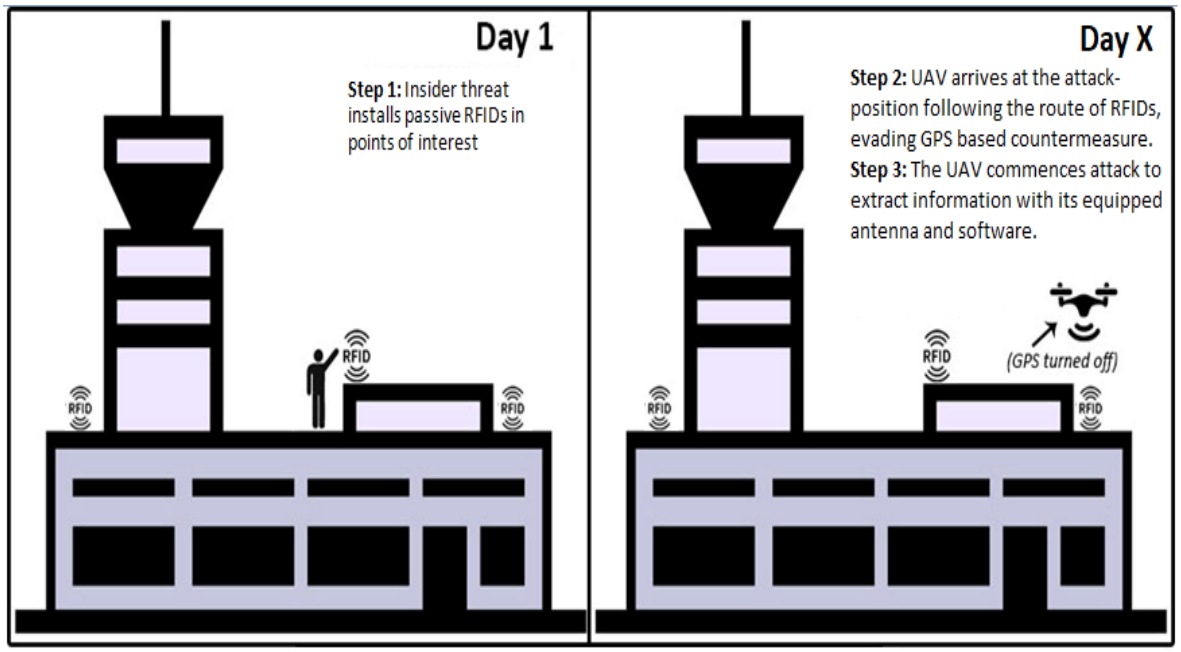

Figure 13: Drone attack in a critical infrastructure, more specifically airport facilities, assisted by insider

Assuming that the critical infrastructure has counter measures against drones and in order for the drone to avoid geofencing, the UAV may turn off its GPS navigation system and follow the route identified by distributed RFID tags, towards its attack-position. As a result, the drone requires less energy to be guided at its destination, relatively to a GPS-navigation based drone, so this expands its flight endurance time. Its small size and low altitude flight can make the UAV untraceable for ground surveillance radars, while anti-drone protection, based on GPS-spoofing, cannot affect its route towards the attack target. If the flight is performed during night time, it can also be untraceable from optical security sensors and human guards.

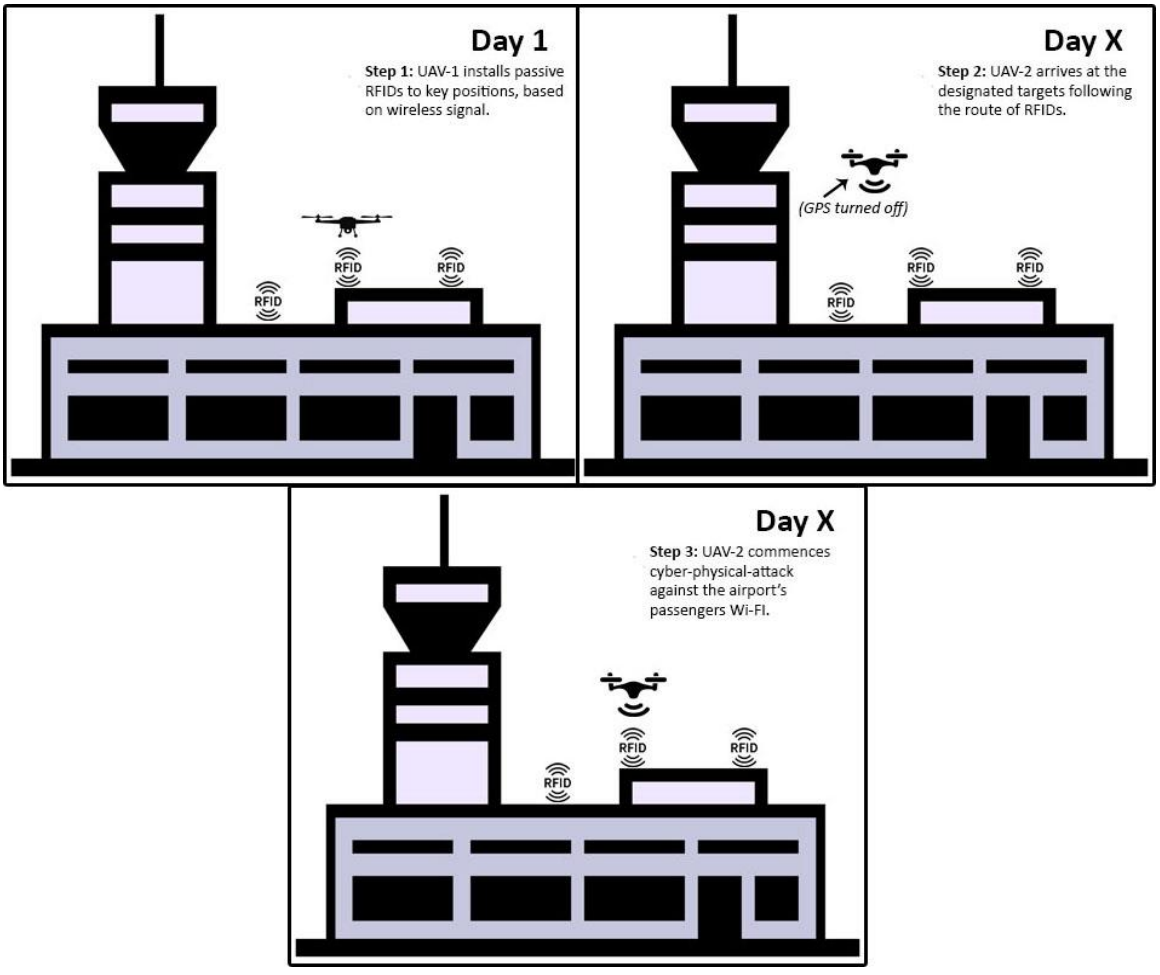

Figure 14: Drone attack in a critical infrastructure, more specifically airport facilities, assisted by RFID drone pre-installation

By following these steps a drone can traverse easily in the same location marked by the RFID beacon and initiate a malicious cyber-attack from the weakest point of a critical infrastructure or from the access point which handles the most critical data of the network. Simultaneously, techniques like signal jamming or data poisoning can be used with better chances of success. This is based on the fact that the proximity of the jamming antenna will increase the power of the jamming signal and hence will increase its effectiveness (which is related to its power) [55], [57]. Additionally the drone can position itself more closely to the clients of an access point and use its stronger signal in order to carry out a "Man in The Middle Attack", a type of attack that, as it was explained at the paper "Main Types of Attacks in Wireless Sensor Networks" [57], the fake access point needs to emit a signal stronger than the original one. Hence the closest positioning is, the greater the success rate for such kind of attack

7 Internet of things in the era of UAS

In this chapter the functionality and mechanisms of Internet of Things (IoT) are presented along with their range of application. Furthermore the liabilities and risk that this technology creates along in combination with the use of malicious drones is analyzed.

7.1 Internet of things (IOT)

Internet of Things or "IoT as it is most commonly known is referring to a interconnected system of mechanical and digital devices which are equipped with a unique identification, while simultaneously be able to transfer data and messages through a distributed network [61] [62].

With the advancement of technology, many fields like embedded systems, machine learning and variety of sensors have shaped the abilities and definition of internet of things enabling to cover a plethora of needs and appliances. Moreover, those mentioned abilities have led to utilization of IoT technology from a variety of everyday devices and appliances. As a result, the IoT can now be found in many homes and almost present in all companies and critical infrastructures [62]. In order to understand the impacts that a malicious cyber-attack may have in IoT system, this chapter is going to shortly present some of their application in critical infrastructures.

1. Medical and healthcare: The devices which use IoT technology and which they are related with the healthcare are not restricted to hospital based medical equipment, but they are also present in the form of sensors onboard the patients [63]. Such devices from automated insulin delivery machines to depression monitors, do posses high risks in the event of a cyber-attack [64].

2. Transportation: In this time and era, the introduction of concepts like "smart cars" and eco-friendly driving, have increased the utilization of IoT devices in cars, while road and traffic-signs are already controlled through a type of IoT [64].

3. Industrial applications: In corporate environments, the term “Industrial Internet Of Things” (IIoT) is used instead of the “IoT”. While its uses extends from cloud computing, to assembly robots to even oil and gas industry in the form of drones which monitor and analyze location too dangerous to be examined by humans, like deep depth pipes etc [66].

4. Aviation field application: Though the IoT is not yet used for coordination between airplanes on air, it is used extensively in the field of aviation safety and service. More precisely, IoT is used in airplane engine and computers diagnostics, a complicate task which requires the communication of multiple devices. Enabling a real-time monitoring and situation awareness of the airplanes functions. Worth mentioning is the fact, that IoT can be found in crew communication and luggage management, both crucial from the aspect of security [67].

7.2 Internet of thing liabilities

The number of devices and services related to the internet of things have rapidly grown to astonishing volumes, it is calculated that they are currently 23 million devices connected in some type of IoT. While it is estimated, that this number is going to increase at more than 76 million by the year 2025 [68]. Moreover, since the IoT is now present from smartphones to automation tools, the risk of cyber-attacks is higher than ever.

According to papers like the “Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things”, the IoT devices have been targeted by a plethora of cyber-attacks [69]. Those cyber-attacks have many similarities with the cyber-attacks related to the Wi-Fi networks since most of the IoT devices communicated through the use of Wi-Fi network.

One of the most common attacks in IoT, is the conscription of the devices to Botnets. Botnets are large interconnected hijacked devices which are used in order to execute commands such flood of ping-messages or email-spamming. A Botnet can be hard to detect from the user, since the only impact on the device can be a slightly slower performance. Hence in IoT devices, the detection is even harder due to the automotive character of the technology (user is not directly in control) [70-71].

Another common attack in the IoT devices, is the Man In The Middle which has be analyzed in the chapter 6. The concept of the attack is the same, but with vital consciousness, since there are reports about cars which they are stolen or even houses robberies which they had taken place with the use of such technique. The culprit behind, is again the lack of direct control from a user and hence the complete "take-over" of the system [70-71].

Data or personal information is also a target in IoT cyber-attacks. The attacker aims to capture messages and packets which they are relayed through the Wi-Fi connection of the IoT devices and then decrypt them in order to gain access on the data. Then use that information in order to deploy further aimed attacks based on the gained knowledge [70], [71]. In order to successfully decrypt the mentioned packets and according to security experts, it takes advantage of common security liabilities of IoT devices like "lack of updates" or "default credentials". Those liabilities were created by the rapidly increase in the number of IoT devices, since the manufactures aim to promote and update only the latest of their models. While at the same time, the users tent to be overwhelmed by the number of devices and hence "abandoned" the live-devices with default credentials [70], [71].

Furthermore, Denial of Service attacks can also be utilized in the same form and manner as explained in the chapter 6, but with the difference that the target will be a corporate distributed IoT, hence taking the name Distributed Denial of Service (DDoS). As has been already explained, in those cyber-attacks the target is not the data or information of the network, but the functionality of the service itself. The corporate IoT will be targeted by a flood of requests, which can be deployed for a botnet residing even in the same company's IoT. The outcome of such attack will be the deactivation of the service and the high complexity of the task of finding the source (i.e. the same network) [70-71].

7.3 UAS and cyber-attacks on IOT

The possibility and sequences of attacks against IoT networks while using as a platform on unmanned aircraft vehicles and systems have been extensively analyzed by researches cybersecurity companies. A paper named "Security Attacks inIoT: A Survey", analyzes and categorizes the attacks that target IoT devices [72], among others it is referring to attacks which rely on the physical position of the attacker.

Physical attacks, also known as cyber-physical attacks, utilize the security liabilities that a system may have it its wireless network due to the confidence that this network is geographical unreachable from the outside world. Such attacks can take the form of already presented cyber-attacks like jamming, data poisoning etc. [72-73], hence no further analyzed is required. Furthermore, such malicious acts take advantage of the architectural design of IoT itself and more precisely the nodes that compose it. According to the paper, a physical attack take place in the form of "malicious node injection" [72-73], in this malicious act, the attacker physically insert a foreign IoT node to the network, it then is able to affect and attack the IoT network from the inside. Hence, a drone can be used in order to position itself insight the IoT network.

Figure 15: The black hat drone which was used as a mean of cyber-attacks against IoT networks [74]

On August 2015, Black Hat company demonstrated how a drone can be used in order to affect industrial scale IoT network [74]. In this presentation by Jeff Melrose, it was proved that even with the limitation in the aspect of battery life and control-accuracy, the drone was able to fulfill its tasks. In the same demonstration, Colin O' Flynn and Eyal Ronen shows that even simple devices like IoT light bulbs can be exploited by utilizing a drone. Based on the aforementioned information and research, along with the chapter 6, the possibility of an attack from an unmanned aircraft vehicle against an internet of things

network is proven and hence realistic. It has also proven that it can be done by utilizing commercially available UAV and technology.

Hence increasing the risk that such malicious act can be manifested by attackers due to the simplicity of the equipment. While at the same time, the severity should such attack take place, is severe and can affect if not disable large in scale critical infrastructure.

8 Brute force and swarm logic

In this chapter the concept of swarm logic and the abilities that may offer in the field of UAV is presented. The chapters continues with an explanation and examples of brute force attacks, while last but not lease the connection and risk of swarm logic, brute force attacks and UAS is analyzed.

8.1 Swarm robotics

Swarm robotics (SR), also commonly known as "swarm intelligence" is a kind of organization and coordination system for robotics and computational devices, inspires by the collectively behavior of insects. In this system, the decision making, and general behavior of the swarm is not directed by a central command module, but rather fabricated by the interaction of each robot with the environment and the other robots which compose the swarm. This collective behavior aims to the simplicity of individual robots as a part of system able to handle complicated missions [75].

The simplicity of the individual robots or drones which comprises by an SR is meant in order to counter the cost and energy requirements of a sophisticated enough robot or drone able to handle the complicate task solely.

Figure 16: Drone light display by Intel [76]

Offering simultaneously scalability (due to the low cost of each unit), easier adaptation in new application (since there is no single expertise robot or drone) and while keeping the ability of executing complicated tasks [75]. Swarm logic applications are many, such as medicine, space exploration etc., yet as a concept is relatively limited to academia usages and "drone light displays" [76].

Though the SR technology has not yet adopted for commercial or industrial usage, they have various models and attempts into creating new services and products based on swarm robotics platforms. An early such example is the "S-bot", a SR robot able to communicate with other robots on the swarm, while at the same time, using collective decision in order to coordinate as a whole [77]. It is based on low-end hardware follows the simplicity rule of the SR system. Moreover, it is able to accomplish complicate task such as passing over a far larger gap with the collectively behavior of the group.

On the same aspect, a paper named "Autonomous Self-assembly in a Swarm-bot", propose the concept of SR system able to construct other robots or even robot-member of the swarm. The paper continuous by presenting a series of task witch the swarm was able to accomplish along with documentation on the software and hardware used [78].

Although the mentioned papers do not address the field o unmanned aircraft vehicles, they can be used to provide a first image of how much SR technology have progressed.

8.2 Brute force attacks

Brute force attack is a type of cyber-attack which aims to "guess" the credentials of a user by utilizing multiple attempts with different username and/or password each time, hence it is an attempt to "crack" the password by providing all the possible combinations witch the criteria given [79],[80]. As a result, the attacker will be able to acquire access in the system by using a legitimate user account, making its detection a complicated task.

Another concept of brute force is based on the fact that the attacker was able to gain access on the encrypted passwords stored insight the system. Early systems were vulnerable to such kind of attacks due to the encryption which was being used like MD5 hashing. The attacker in them mentioned possibility, utilize brute force attacks on the acquired file itself rather than the system from which have gained it. Once the encryption in cracked, the attacker use the credential and gains access on the system [79].

Due to the calculation and nature of brute force attacks, it requires large computational power over an equal lengthy time in order to crack the encryption or find the credentials directly. Hence such types of attacks are categorized as time consuming with larger passwords while at the same time is quite effective when is used against smaller passwords [79-80].

Furthermore, they are many types of brute force attack which are distinguished based on the techniques they utilize. A dictionary attack is a type of cyber-attacks which uses combination drawn from a dictionary instead of using all the possible combinations. This dictionary contains words that most commonly found in the user's passwords. Additionally, a dedicated dictionary can be constructed based on the personal information of the user known to the attacker (i.e. surname, name, date of birth etc) [79]. Those types of attacks do have a limitation due to the same dictionary they use in order to speed up the process. That is that if the user has a non-common password combination or not in relation with his known personal information, then the dictionary would now contain a proper combination. As a result, the attack will fail after it has tried of the words and combination present in the dictionary.

Rule based attacks, use the same conception as the dictionary attacks, but in this type, instead of a dictionary, an algorithm which produces combinations is used. This algorithm utilizes personal information of the user and then generate password base on pre-calculate rules. The rules are based on the password patterns that can be found in most common use, creating in this way a template for password creation. Hence, the generated password can be variation of the user's personal information or a combination of them with often found in password words [80-81].

8.2.1 Brute force attack requirements

Along with the evolution of cybersecurity and acceptable credentials, the computational needs in order to crack the password with one of the mentioned types of brute force have increased exponentially [1]. This effect though, had been countered by the exponentially increase in the computational power which an attacker can gain access with relative cheap price. Hence a cyber-attack of the brute force type, can be used and complete successfully in a reasonable amount of time [79], [82-83].

Elcomsoft, an enterprise dedicated to security, have released an article in which a NVIDIA GPU was used in order to speed up the calculation needed for a brute force attack 824]. The same article presents the concept, that GPUs can produce far faster results then CPUs should they used for brute force attacks. The mentioned outcome reached a factor of over 100 times faster than CPU which can be bought in the same price. Furthermore, it states they are much more efficient way from power consumption perspective than the CPU counterpart. The same article, explains that the number of cores play a significant part in the time needed for a brute force attack.

On the same aspect, a paper with the title "Effective uses of FPGAs for brute-force attack on RC4 ciphers" is examining the effectiveness which a Field Programmable Gate Array (FPGA) may have if used for a brute force attack. The research paper continues by presenting the results of a brute force attack against an RC4 encryption [83].

The above-mentioned reference though does not direct mentioning that the technologies can be used on UAV, it paves the way since it is presents that a low cost and low energy hardware solution can be used in order to implement a brute force with it. Worth mentioning, is the fact that the paper proved that it can be done from a solely FPGA unit [83]. In the next chapter further information regarding the implementation of such attacks are going to be presented.

8.3 UAS, Swarm robotics and brute force attacks

Swarm robotics is a technology already present and with practical implementation in the field of unmanned aircraft systems. Many researches have exploited the usage which such technology may have in the UAS implementations [84-85].

The paper named "Modelling Oil-Spill Detection with Swarm Drones" presents at system which utilize drones integrated into a swarm network and with the task of the detection of Oil spills in the oil industry. The research article proposes that a system of SR drones is able to locate and monitor an oil leakage with far greater accuracy and results. Moreover the simplicity of each independent drone, enables for a cheaper and easier maintenance as a whole system [84]. Another paper with the name "UAV Swarm Mission Planning and

Routing using Multi-Objective Evolutionary Algorithms", examines the introduction and use of complicated root algorithms to SR drones [84].

Though the mentioned papers does not cover the cybersecurity aspect, they do prove that the SR technology in unmanned aircraft vehicle is mature enough to accommodate practical usage [84], while simultaneously able to correspond to complicated algorithms and tasks [85].

Figure 17: A photo in which the WASP and part of its interior is shown [86]

Mike Tassey and Richard Perkins present their UAV named Wireless Aerial Surveillance Platform (WASP) at the at the Black Hat and Defcon security conference [87]. Their drone, was capable among others to perform brute force attacks and specifically dictionary attacks. Even though the UAV utilize a Linux operating system computer with a size of a few centimeters, it was able to crack/guess the password of 11 antennae.

Based on the aforementioned information and according to the articles and research paper presented, the threat of unmanned aircraft system able to utilize both swarm robotics technology and brute force attack is possible. A SR drone can have multiple cores for each and every drone which is part of the swarm. As it was already explained, the number of

cores may have the same outcome as the computational power when applied for brute force attacks. Thereby, low-end drones which compose a swarm can be used for brute forces as it was proved by the related article [87].

Therefore the paper propose the idea of possible cyber-attack from SR drones which can utilize the multiple cores present in the swarm in order to launch brute force attacks. The outcome which such attack many have in critical infrastructure have already been presented in the related chapters.

9 UAS security challenges

In this chapter UAS detection technologies along their capabilities and restrictions are presented, followed by an analysis at possible countermeasures currently used against drones. The chapter continuous by presenting the popular concept of using drones as countermeasures themselves.

9.1 UAS detection

Another method of cybersecurity for critical infrastructures and especially in the aviation sector (which host large open spaces and roofs) is the detection of the drone and prevention of it to enter the premises of the infrastructure [88], [93]. According to a research paper named "Micro-UAV Detection and Classification from RF Fingerprints Using Machine Learning Techniques", the method used to detect a drone, can be categorized in four types. The classification is based on which technology is used in order to cope with the task of detection [88].

The first category of detection is the "Radar-based techniques", which uses the well known radar technology in order to localize and track an object. This is achieved with the use of electro-magnetic waves transmitted from an antenna. The waves will be reflected from the surface of the object and a receiving antenna (usually the same which emits the waves) will capture the reflected waves. By analyzing the factors like time and wave strength, the system is able to calculate with great accuracy the position of the object [88-89].

For smaller object, like unmanned aircraft vehicles, the radar utilize the Doppler Effect in order to distinguish the kind of the object. Doppler Effect is the distortion of the frequency of a carrier signal due to the velocity of the receiver. Moreover, a technique which utilizes the "micro-Doppler effect", which is the distortion of the frequency of the signal due to the vibration etc. characteristics of the reflection area, can also be used. The mentioned technique offers additional information regarding the target such the type of propulsion or number of engines [88-89]. Papers like the "Classification of small UAVs and birds by micro-Doppler signatures", have utilized the mentioned technology in order to be able to locate and track a small UAV and even be able to distinguish it from an object which papers with the same radar signature such as birds [90].

The second category of detection is the “Sound-based Techniques”, which utilize an array of sound sensor/microphones in order to collect and monitor sounds present in the specified airspace. The data which have been collected can then be analyzed in live time in order to remove the background noise and distinguish the sounds which are produced form the motors of the unmanned aircraft vehicles [88].

That can be achieved due to the fact that the UAVs’ electro motors, produce a buzz-like sound in the frequency range from 400Hz to 8kHz. While their present can be found with the explained technique, the estimated location of the drone can be calculated based on the time difference of arrival of the sound to the different microphone [88].

Systems which utilize the mentioned technique for UAV detections like the “Real-time UAV sound detection and analysis system” use the same bases enhancing them with machine learning in order to produce greater accuracy [4]. While papers like the “Low-Cost Acoustic Array for Small UAV Detection and Tracking”, have produced low cost systems able to detect and locate small UAV [92]. As a result such arrays can be used in larger number improving the prevention capabilities of a system.

The third category of detection is the “Vision-based Techniques”, which high and very high resolution camera are utilized in an array configuration order to capture subsequent pictures of an area [88]. The images are then used as an input in a deep learning network in order for the classification to take place. The deep learning network is able to detect unmanned aircraft vehicle and keep track of it based on the image which is provided with. Another technique implements the same conception but by utilizing convolution neural network instead of deep learning network. Though both techniques are capable of monitoring an area with good performance ratio, their usage requires high end equipment and high computational power, making it an expensive solution [88].

A paper called “Vision-Based Detection and Distance Estimation of Micro Unmanned Aerial Vehicles“, presents a system which is able to detect UAV and even micro-UAV in the premises of an infrastructure, by utilizing vision algorithms [93]. The system also integrates a distance estimation procedure in order to provide the distance of the drone as part of the solution.

The fourth and last category of detection is the “RF fingerprinting”, which the RF signal produced by the controller and the UAV is used in order to detect and identify a drone [88]. As the study mentions, the RF signals which are transfer between the controller and

the UAV, do possess a characteristic and unique RF signature, hence the name "RF fingerprint". The mentioned type, possess the best energy efficiently due to the passive antenna which use in order to capture the RF signals. The most worth mentioned ability of this class, is that in can cope with the extremely hard to detect micro UAVs since it is aims to detect and intercept the controller without the need of finding the drone itself.

RF fingerprinting also offers high operational range, which a crucial problem in the second and third category. This is due to the fact that high sensitive antennas can be used in relatively low cost. The "Micro-UAV Detection and Classification from RF Fingerprints Using Machine Learning Techniques" paper [88], presents the concept of an improved RF fingerprint detector with enhanced capabilities based on supervised machine learning.

9.2 UAS counter measures

The need for quick and effective response against possible malicious or malicious drones has created a plethora of countermeasures [94]. Moreover, the need was so crucial that lead to the adaptations of countermeasures integrated to the drones by the manufactures in the form of "geofencing".

Geofencing is the creation of a virtual barrier by utilizing information of the geographical petition of the drone (through GPS) or by low radio frequency identifiers (LRFID). The dimensions and position of the geofence along with the classification of the territory is handled by software pre-installed in the drone from the manufacturer [95]. The drone software will recognize that the given position is restricted and hence in would not enter it. Though this method is quite effective for regular user, in the case of a more expert hacker could be by-passed with the GPS spoofing techniques such the ones presented in the previous chapters [94]. Furthermore, open-source software which implements the above method is well spread-out in the internet and well documented [94].

A more sophisticated kind of countermeasures is relying on the hacking technique presented at chapter 3 [94]. More precisely counter measures in the form of attacks on the control communication stream and data communication stream can be implemented. As a result the suspected drone can be forced down or disable its capabilities of flying and relaying information back to the controller. In similar way control commands from the

controller can be nullified (chapter 3). In similar bases, anti-drones' systems like the one presented in the state of the art chapter, can use spoofing type attacks in order to gain control over the drone and force it to land in a specific safe location.

Such kind of methods are called as "Electronic defenses" and they effectives can be nullified if the attackers have set their drone in a so called "radio silence mode" [94]. In this custom-made mode, the unmanned aircraft vehicle software is alternate in such ways that do not require to receive of any kind of signal from the controller. In other words, after the takeoff, the UAV does not enable its antenna-receiver, hence the drone will only execute a set of predefined commands. The same approach can be applied form the aspect of GPS, nullifying the GPS-spoofing based counter-attacks [94] [chapter].

Should all the mentioned countermeasures failed to stop the UAV from entering a restricted airspace, kinetical type of measures can be used in order to hinder the flight of the drone [94]. Those kinetic defense, utilize means like bullets from soft materials like rubber, guns that deploy nets or even stronger weaponry like shotgun shots. Their drawback is that their excess power can destroy a false believed to be malicious drone, destroy evidence or even cause the detonation of the payload of the drone [94].

Last but not least, worth mentioning is the idea of utilizing the already present system which utilize large predator birds like eagles in order to keep small birds in distance from an airport. This countermeasure is not optimal and can result in harm for the pray-bird itself as well stated by the paper "How to evaluate counter-drone products" [96]. Nevertheless, it can be used as a stop gap measures for airports without the proper equipment for a technological oriented solution [96]

9.3 UAS as countermeasures

In the recent year, the idea of utilizing unmanned aircraft systems as a countermeasure to hostile or suspected drones have been introduces and implemented by some states. The drones can be equipped with a variety of sensors able to help in detecting and tracking a rogue drone. Such sensors include vision sensor, acoustic sensor and even mobile radar detectors, increasing the effectiveness of the counter-drone [88] [97] [99]. The Tokyo police have adopted such an idea and have acquired a fleet of drones able to detect and track drones which flying in restricted areas. The police drone is equipped with a camera

for monitoring and a suspended net which hover under the drone. The scope is that the police drone will guide its equipped net against the rogue drone, capture it insight the net and force is to the ground in a safe and secure manner.

Figure 18: A drone used by the Tokyo police in order to capture mid air a suspect drone [98]

Additionally, a security company name “Dutch firm Delft Dynamics” has lanced the idea of a UAV quadcopter able to shoot nets on the target drones instead of a pre-deployed net. Their creation is called DroneCatcher and it is able to use a variety of sensors like the ones already described [99]. The net is able to be launched effectively at a distance of 20 meters while cord reconnected to the DroneCatcher, will keep the net along the captured drone suspended in the air. By implementing this technique, the malicious drone is protected from a potential hazardous fall to the ground. The company took a step in the evolution of the drone and added a ground connected cable which allows the drone to draw power from it. As a result, the drone can stay airborne indefinite, scanning and protecting against drones. Once a rogue drone is detected, the «DroneCatcher» release the power cable, switch to its battery as power source and initiate the pursue of the malicious drone [99].

10 UAS and Smart airport

In this chapter the concept and categorization of airports and smart airports is presented. The chapter continuous with the analysis and presentation of the cybersecurity liabilities which the smart airport posses along with the role of UAS in cyber-attacks.

10.1 Smart airports

According to "Airport Council International" (ACI), the annual world airport traffic for the year 2018, was more the 8.3 billion passengers while the cargo transferred by the air reached more than 118 million of metric drones [100]. Those numbers do not only show the huge volume of passengers and cargo transfer through the aviation field, but also depict an increase of 7.5% and 7.7% respectively from the year 2017. ACI estimates that the number of passengers traveling by air will surpass the 20 billion by 2040.

Based on those statistics and prognosis, many private companies and research institutes have studied the next step in the aviation sector and more precisely the analysis and implementation of smart airports. Following the evolution of the airports, they can be distinguished into three categories [101]

1. Airport 1.0 (Basic Airport Operations): Which can handle basic airport operations like the necessary safety features along with an efficiency in handling passengers and cargo [101].

2. Airport 2.0 (Agile Airports): Those airports cover the services provided by the previous category, but they are enhancing them with new technologies in response to the quick changing environment. They accommodate web services like Wi-Fi, video surveillance etc. both for the passengers and working personal [101].

3. Airport 3.0 (Smart Airports): Those airports cover the services provided by both the previously mentioned categories, while extending the capabilities, security measures and services. This is accomplished by utilizing the emerging and state of the art technologies [101].

According to the paper "Smart Airports: Transforming Passenger Experience To Thrive in the New Economy", a smart airport incorporates technologies which are centralized and communicate through a "digital grid". The mentioned digital grid, is acting as the central point of command of the airport, effectively managing every interaction and information. That information will be extracted from a series of sensors and cross-references of their readings. It will also serve as an interaction point for all the passengers and working personnel [101].

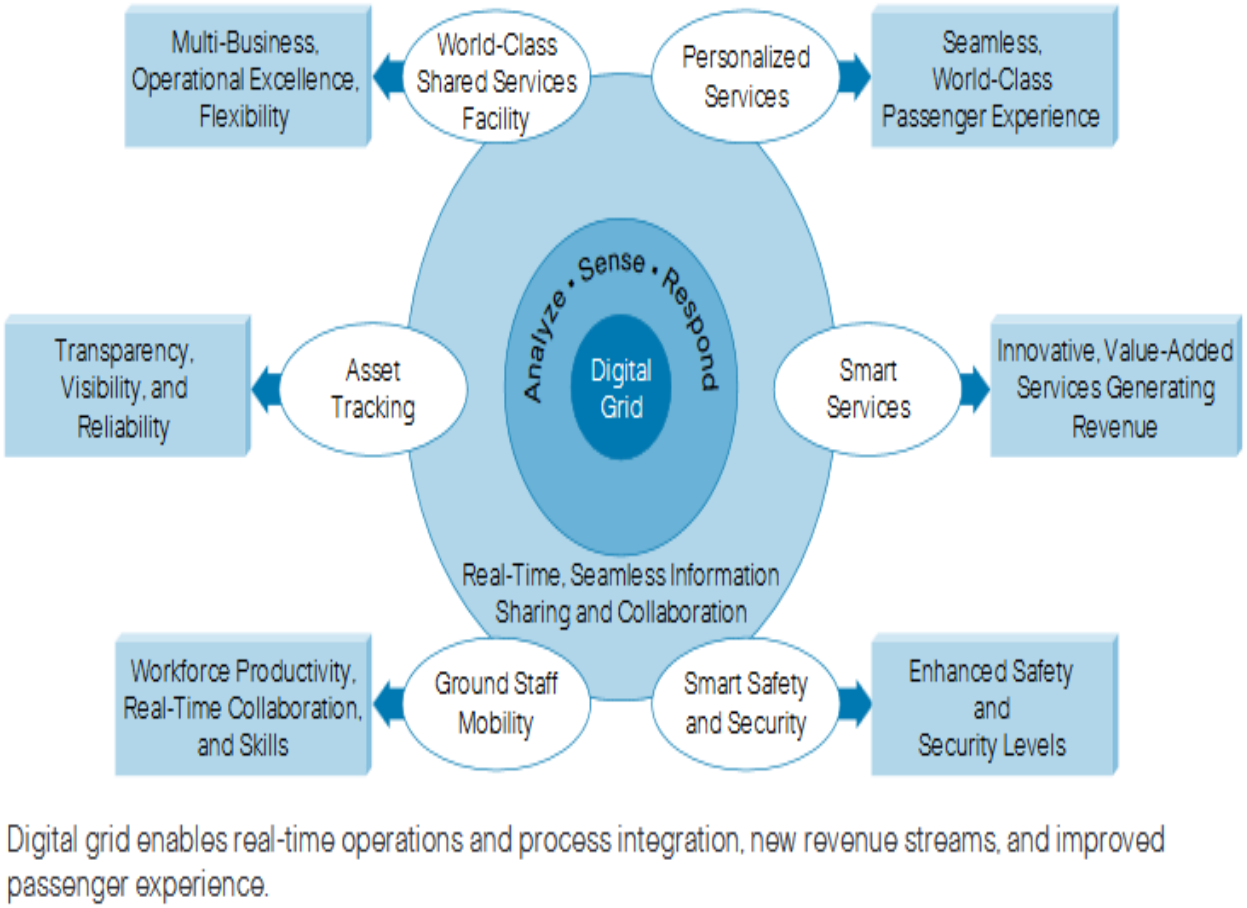

Figure 19: The vision of a smart airport as presented in the paper "Smart Airports" [101]

According to the study "Intelligent Airports - Your runway to success", a smart airport should accommodate technologies such as biometric sensors, ability to track and trace both personal and passengers, ability to track and trace both cargo and passengers' packages, be able to analyze the video surveillance data and even have smart healthcare services [102].

10.2 Smart airport cybersecurity

Cybersecurity is a crucial part in every airport in order to sustain its services, security features and efficiency [104]. This aspect is closely connected with the APOC, according to a study published by the Single European Sky ATM Research (SESAR) which is the European air traffic control infrastructure modernization program [104]. The APOC stands for Airport Operations Centre and is essential the central network which handles all the decisions and processes from flight control to ground handlers. In other words, the APOC is essentially the "digital grid" which was analyzed in the previous chapter.

Though those breakthrough technologies have led to the introduction of smart buildings and airports, it also created a whole new sector of security liabilities and cybersecurity, according to the same study [104]. Simultaneously, the integration of heterogeneous data sources offers a more holistic picture over the operations that taking place, hence it creates opportunities and prerequisites for a more improved cyber-defense which is based on an mutual conception. As a result, it is vital for the inputs taken, to be reliable along with the outputs provided by the system.

The cyber-liabilities that the implementation and usage of such "digital grid" creates or will have to defend from can be categorized in 8 types [104]:

1. Insider threats: Those are personal with legitimate access to the APOC.

2. Hacktivists: Which are people who fight for ideological motives.

3. Hacker and or virus writers: Who find entrainment in such malicious acts

4. Business competitors or/and foreign intelligent services: Which are motivated from the economic or other advantage that their country or company may gain.

5. Cyber-criminals: Who will try to gain economic gains through their cyber-attacks and frauds.

6. Terrorists: Who will try to obtain sensitive information

7. Organized crime: Which has as a target to obtain financial gains in the form of ransom or rewards.

8. State Cyber-Forces: Who aim to disrupt or destroy national critical infrastructure.

The study points out that without a variety of detailed insider information regarding the implementation of the system, a cyber-attack will only be able to accomplish a minor outcome. Furthermore, the attackers will also need to be highly organized and with significant funds available [104].

According to another article titled “Smart Airport Cyber-security: Threat Mitigation and Cyber Resilience Controls” [2], a smart airport should be prepared for cyber-attacks which use as their base technologies like IoT and smart devices connected at its network. The paper continuous by extensively analyzing and presenting the plausible cyber-attacks that must be covered, while simultaneously categorizing them in 5 main categories.

1. Network and Communications attacks: Which are attacks aiming the network and categorized in active and passive attacks 105].

2. Malicious software: Which are malwares able to infect both the systems and the smart devices connected to it [105].

3. Tampering with Airport smart devices: Which included the manipulation of data stored, systems and sensor data which are drowned from the smart devices [105].

4. Misuse of authority: Which includes stolen authorization credentials or insider threads [105].

5. Social and Phishing attacks: Which is the manipulation of unwary people in order to perform actions that will help the attacker, such us sharing credentials of the airport Wi-Fi [105].

10.3 UAS cyber-attacks in smart airports

Based on the previous chapters, the use of unmanned aircraft vehicles and systems in the aviation sector has been already introduced and adopted in a variety of different applications. Simultaneously, the new services that the further implementation of UAV may offer is more than promising and according to the studies is the next evolutional step of smart airports. Canard Drones offers services to airport, in which the vital act of calibration of airstrip beacons is been made with the use of drone [21]. As a result, the aviation sector and specifically the airports will need to adapt in both cybersecurity against drones and in the cybersecurity of the drones utilizing by the system of the airport.

More precisely, as it was already presented in the previous chapter, smart airports and agile airports do offer services in their passengers by utilizing technologies like IoT and Wi-Fi networks. The same technologies are also used from the system and personal of the airport. Hence, a cyber-attack on those assets can posses serious outcomes in the functionality and services of the airport. Both IoT and Wi-Fi networks can be exploited with the use of drones and even affect directly the smart devices of the passengers.

Cyber-attacks like those mentioned in the “chapter 3” and “chapter 4”, can be utilized in order to map and tag the airport and the nodes of the system, while 3D-maps can offer valuable info in every cyber or conventional attack. Moreover with the large number of IoT nodes and Wi-Fi communication, liabilities in the system can be created. Black Hat demonstrated, that drone can used to exploit IoT devices like the ones that can be found in an airport. Simultaneously, in the same chapter, more complicated malicious acts like node injections etc. have been proved to be able to be accomplished by drones in critical infrastructures.

Though the study “Addressing airport cybersecurity” mentions that such attacks cannot be done without inside level of information, the crucial outcome which may result from a cyber-physical attack against an airport, sets the necessity for counter-security to levels that cannot be ignored.

11 Conclusions

Throughout the human history, it was always the small steps that lead to technological revolutions; Unmanned Aircraft Systems are no different and with them came a new era in nearly every aspect of our society. Ranging from monitoring, marketing usage, military, search and rescue, entertainment etc, UAS have gone hand to hand with a technological revolution in each and every field; and cybersecurity is no exception.

Critical infrastructures including but not limited to airports, factories and banks, are fields that have already been targeted from UAS in the form of cyber-attacks or cyber-physical-attacks, while simultaneously such attempts are expected to increase dramatically following the rapid increase of UAS numbers. Many of those Unmanned Aircraft Systems have been produced without safety considerations from both legal and cybersecurity aspect. Moreover, the rapid transition to cheaper and improved versions of drones has introduced an increase in active drones that do not get security updates, even though their vulnerabilities are publicly available.

In addition, the World Wide Web is full of information regarding the use, manufacture or reconfiguration of drones, information which can be used for malicious acts. Based on the papers presented during this thesis, the abilities that such drones possess can easily target a plethora of different devices and critical infrastructures. The attack scenarios presented in this paper have also proved that complicated and unforeseen till now cyber-physical-attacks can be accomplished with relatively cheap and commercially available drones and electronic parts.

Counter measures against UAS have already encapsulated a variety of different approaches regarding the detection, identification and immobilization of drones. Larger drones can be easily detected with radars, acoustic or vision based sensors, while smaller drones and micro UAVs require the usage of specialized radars, rf-detection or enhanced acoustic sensors. Regarding the counter measures, technologies like geo-fences, restrain nets, jamming or even drones can be used as already analyzed.

On the contrary, counter UAS technology still poses a wide range of practical, legal, and policy challenges in a civilian dominated environment. Efforts to identify new methods that will protect large areas of airspace are ongoing, Remote Identification requirements for civilian drones being under design, while simultaneously the users' legal private information are delimitated.

As a result, critical infrastructures must adopt a security policy which incorporates UAS based attacks, along with the needed detection technologies, counter measure equipment and proper personnel training. Such equipment can be deemed as too expensive or not fully proofed when it is applied in large areas, hence, additional cybersecurity policies against cyber-physical-attacks must be planted and implemented.

However, defending critical infrastructures against malicious drone cyber-activity is a wide and significant complicated problem set. Although there is a number of technological mitigation solutions, CI must remain within the law, when using disruptive technologies, and the risks on the wider community should be fully assessed and understood. Any decisions against a flying object should be appropriate, proportionate and necessary with documentation along with the rationale for making it. Furthermore, appropriate responses must taken by the security personnel before, during and immediately after any UAV incident, creating a security culture with orientation to continuous evolution and action.

"Computers are like Old Testament gods; lots of rules and no mercy."

Joseph Campbell

12 Reference / Links

1. Loukas, G., 2015. *Cyber-Physical Attacks, A Growing Invisible Threat*. 1st ed. Butterworth-Heinemann.

2. Pentestpartners.com. 2020. *Sinking A Ship And Hiding The Evidence*. [online] Available at: <https://www.pentestpartners.com/security-blog/sinking-a-ship-and-hiding-the-evidence/> [Accessed 13 November 2019].

3. Pritchard, S., 2019. *Drones Are Quickly Becoming A Cybersecurity Nightmare*. [online] Threatpost.com. Available at: <https://threatpost.com/drones-breach-cyberdefenses/143075/> [Accessed 21 November 2019].

4. Paganini, P., 2015. *Zigbee-Sniffing Drone Used To Map Online Internet Of Things*. [online] Security Affairs. Available at: <https://securityaffairs.co/wordpress/39143/security/drone-internet-of-things.html> [Accessed 13 November 2019].

5. Wilkinson, G., 2014. *Digital Terrestrial Tracking: The Future Of Surveillance*. [ebook] DefCon. Available at: <https://pdfs.semanticscholar.org/07a5/08ddd6cc3eadd1f0743e7acf8a38db467703.pdf> [Accessed 14 November 2019].

6. Gittleson, K., 2014. *Snoopy Drone Sniffs Public's Data*. [online] BBC News. Available at: <https://www.bbc.com/news/technology-26762198> [Accessed 2 November 2019].

7. Dulo, D., 2015. *Unmanned Aircraft: The Rising Risk Of Hostile Takeover [Leading Edge]*. [ebook] IEEE Technology and Society Magazine. Available at: <https://ieeexplore.ieee.org/document/7270428> [Accessed 15 November 2019].

8. Krishna, C. and Murphy, R., 2017. *A Review On Cybersecurity Vulnerabilities For Unmanned Aerial Vehicles*. [ebook] IEEE Technology and Society Magazine. Available at: <https://ieeexplore.ieee.org/abstract/document/8088163> [Accessed 3 December 2019].

9. Mansfield, K., Eveleigh, T., Holzer, T. and Sarkani, S., 2013. *Unmanned Aerial Vehicle Smart Device Ground Control Station Cyber Security Threat Model*. [ebook] IEEE Technology and Society Magazine. Available at: <https://ieeexplore.ieee.org/abstract/document/6699093> [Accessed 18 November 2019].

10. S. Salamatian, W. Huleihel, A. Beirami, A. Cohen and M. Médard, "Why Botnets Work: Distributed Brute-Force Attacks Need No Synchronization," in *IEEE Transactions on Information Forensics and Security*, Available at: < https://ieeexplore.ieee.org/abstract/document/8629000 > [Accessed 13 December 2019].

11. Fortinet, 2018. *Swarm Cyberattacks Target The Internet Of Things (Iot) With Growing Intensity*. [online] Available at: <https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2018/threat-landscape-report-reveals-attacks-per-firm-increased.html> [Accessed 29 November 2019].

12. Martens, D., Baesens, B. and Fawcett, T., 2010. *Editorial Survey: Swarm Intelligence For Data Mining*. [ebook] Springer. Available at: <https://link.springer.com/content/pdf/10.1007/s10994-010-5216-5.pdf> [Accessed 17 November 2019].

13. Hasan, Y., 2017. Swarms Intelligence and Their Applications in Data Mining. *IOSR Journal of Electrical and Electronics Engineering*, [online] Available at: <https://pdfs.semanticscholar.org/c055/a93c09b72153d48b2d38655b58bd1736a642.pdf> [Accessed 25 November 2019].

14. Trieu, K. and Yang, Y., 2018. Artificial Intelligence-Based Password Brute Force Attacks. *MWAIS 2018 Proceedings*, [online] Available at: <http://aisel.aisnet.org/mwais2018/39> [Accessed 13 December 2019].

15. Soare, B., 2019. *Cybersecurity And Drones - A Rising Threat?*. [online] Heimdal Security Blog. Available at: <https://heimdalsecurity.com/blog/cybersecurity-drones/> [Accessed 20 December 2019].

16. European Commission, 2018. *Protecting People And Sites From Malicious Drones*. [online] Available at: <https://ec.europa.eu/research/infocentre/article_en.cfm?id=/research/headlines/news/article_18_11_07-1_en.html?infocentre&item=Countries&artid=49757&caller=SuccessStories> [Accessed 18 November 2019].

17. Shattil, S. and Sen, R., 2018. *US10051475B2 - Unmanned Aerial Vehicle Intrusion Detection And Countermeasures - Google Patents*. [online] Patents.google.com. Available at: <https://patents.google.com/patent/US10051475B2/en> [Accessed 12 November 2019].

18. Terwilliger, B., Vincenzi, D., Ison, D., Witcher, K., Thirtyacre, D. and Khalid, A., 2015. Influencing Factors for Use of Unmanned Aerial Systems in Support of Aviation Accident and Emergency Response. *Journal of Automation and Control Engineering*, [online] Available at: <http://www.joace.org/uploadfile/2014/0930/20140930111743966.pdf> [Accessed 10 November 2019].

19. Farhan, M., Nader, M. and Jameela, A., 2014. UAVs for smart cities: Opportunities and challenges. *2014 International Conference on Unmanned Aircraft Systems (ICUAS)*, [online] Available at: <https://www.researchgate.net/profile/Nader_Mohamed/publication/269299864_UAVs_for_smart_cities_Opportunities_and_challenges/links/561fc12108ae93a5c9242365/UAVs-for-smart-cities-Opportunities-and-challenges.pdf> [Accessed 13 December 2019].

20. Yang, S., Ceylan, H., Gopalakrishnan, K. and Kim, S., 2014. Smart airport pavement instrumentation and health monitoring. *Civil, Construction and Environmental Engineering Conference Presentations and Proceedings. 8.*, [online] Available at: <https://lib.dr.iastate.edu/ccee_conf/8> [Accessed 19 November 2019].

21. Carnard Drones, 2020. *Smart Drones For Smart Airports*. [online] Available at: <http://www.secpho.org/wp-content/uploads/2017/03/23-CANARD_DRONES_Presentacion_SECPhO_Cluster-aeroespacial.pdf> [Accessed 13 November 2019].

22. Fahlstrom, P. and Gleason, T., 2013.*Introduction To Uav Systems*. Hoboken, N.J.: Wiley.

23. Keane, J. and Carr, S., 2013. A Brief History of Early Unmanned Aircraft. *Johns Hopkins APL Technical Digest*, [online] Available at: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.686.7958&rep=rep1&type=pdf> [Accessed 13 January 2020].

24. Buckley, J., 2006. *Air Power In The Age Of Total War*. London: Taylor and Francis.

25. Merriam-webster.com. n.d. *Drones Are Everywhere Now - But How Did They Get Their Name?*. [online] Available at: <https://www.merriam-webster.com/words-at-play/how-did-drones-get-their-name> [Accessed 14 January 2020].

26. Ctie.monash.edu.au. 2005. *Reginald Denny (1891-1967) - Aviation Pioneer*. [online] Available at: <http://www.ctie.monash.edu.au/hargrave/dennyplane.html> [Accessed 3 January 2020].

27. Vyas, K., 2018. *A Brief History Of Drones: The Remote Controlled Unmanned Aerial Vehicles (Uavs)*. [online] Interestingengineering.com. Available at: <https://interestingengineering.com/a-brief-history-of-drones-the-remote-controlled-unmanned-aerial-vehicles-uavs> [Accessed 5 January 2020].

28. Federal Aviation Administration, Small Unmanned Aircraft System (UAS) Aviation Rulemaking Committee, 2008. *Small Unmanned Aircraft System Aviation Rulemaking Committee*. [online] Available at: <https://www.faa.gov/regulations_policies/rulemaking/committees/documents/media/SUASARC-4102008.pdf> [Accessed 12 January 2020].

29. Desjardins, J., 2016. *Here's How Commercial Drones Grew Out Of The Battlefield*. [online] Business Insider. Available at: <https://www.businessinsider.com/a-history-of-commercial-drones-2016-12> [Accessed 9 January 2020].

30. Dronethusiast. 2019. *Drone Companies To Watch 2020 (Best New Drone Companies)*. [online] Available at: <https://www.dronethusiast.com/drone-companies/> [Accessed 11 January 2020].

31. Wall, M., 2019. *Propelling Exploration: Drones Are Going Interplanetary*. [online] Space.com. Available at: <https://www.space.com/nasa-drone-exploration-dragonfly-mars-helicopter.html> [Accessed 8 January 2020].

32. Logan, M., Chu, J. and Motter, M., 2020. Small UAV Research and Evolution in Long Endurance Electric Powered Vehicles. [online] Available at: <https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20070021697.pdf > [Accessed 8 January 2020].

33. Dormehl, L., 2018. *7 Drones With Super Long Flight Times*. [online] Digital Trends. Available at: <https://www.digitaltrends.com/cool-tech/drones-with-super-long-flight-times/> [Accessed 14 January 2020].

34. Mogg, T., 2018. *This Drone Is A 'Flying Battery' Than Can Stay In The Sky For 2 Hours*. [online] Digital Trends. Available at: <https://www.digitaltrends.com/cool-tech/impossible-aerospace-us-1-flying-battery-drone/> [Accessed 12 January 2020].

35. The first petrol-electric multicopter. [online] Quaternium. Available at <https://www.quaternium.com/uav/hybrix-20/> [Accessed 8 November 2019].

36. Brown, J., 2016. *Gas Powered Quadcopters: Best Models Overview*. [online] My Drone Lab. Available at: <https://www.mydronelab.com/blog/gas-powered-quadcopter.html> [Accessed 13 January 2020].

37. Seo, S., Lee, B., Im, S. and Jee, G., 2015. Effect of Spoofing on Unmanned Aerial Vehicle using Counterfeited GPS Signal. *Journal of Positioning, Navigation, and Timing*, [online] Available at: <https://www.researchgate.net/publication/283006977_Effect_of_Spoofing_on_Unmanned_Aerial_Vehicle_using_Counterfeited_GPS_Signal> [Accessed 8 January 2020].

38. Rani, C., Modares, H., Sriram, R., Mikulski, D. and Lewis, F., 2015. Security of unmanned aerial vehicle systems against cyber-physical attacks. *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*.

39. Friedberg, S., 2018. *A Primer On Jamming, Spoofing, And Electronic Interruption Of A Drone*. [online] Dedrone.com. Available at: <https://www.dedrone.com/blog/primer-jamming-spoofing-and-electronic-interruption-of-a-drone> [Accessed 14 January 2020].

40. Das, R., 2020. *RFID Forecasts, Players And Opportunities 2016-2026: Idtechex*. [online] Idtechex.com. Available at: <http://www.idtechex.com/en/research-report/rfid-forecasts-players-and-opportunities-2016-2026/451> [Accessed 25 January 2020].

41. Landt, J., 2005. The history of RFID. *IEEE Potentials*, [online] Available at: <https://web.archive.org/web/20090327005501/http://www.transcore.com/pdf/AIM%20shrouds_of_time.pdf> [Accessed 26 January 2020].

42. Want, R., 2006. An Introduction to RFID Technology.*IEEE Pervasive Computing*, [online] Available at: <https://www.cs.colorado.edu/~rhan/CSCI_7143_002_Fall_2001/Paper/rfid_intro_01593568.pdf > [Accessed 26 January 2020].

43. Swedberg, C., 2018. *Active RFID Goes Overhead With Drone-Based Reader | RFID JOURNAL*. [online] Rfidjournal.com. Available at: <https://www.rfidjournal.com/active-rfid-goes-overhead-with-drone-based-reader> [Accessed 28 January 2020].

44. Greco, G., Lucianaz, C., Allegretti, M. and Bertoldo, S., 2015. Localization of RFID tags for environmental monitoring using UAV. *IEEE*, [online] Available at: <https://www.researchgate.net/publication/308463746_Localization_of_RFID_tags_for_environmental_monitoring_using_UAV> [Accessed 27 January 2020].

45. Hardesty, L., 2017. Drones relay RFID signals for inventory control. [online] MIT Available at: < http://news.mit.edu/2017/drones-relay-rfid-signals-inventory-control-0825 > [Accessed 6 January 2020].

46. Cipra, B., 1999. *Engineers Look To Kalman Filtering For Guidance*. [online] Cs.unc.edu. Available at: <https://www.cs.unc.edu/~welch/kalman/siam_cipra.html > [Accessed 8 January 2020].

47. Dissanayake, M., Newman, P., Clark, S., Durrant-Whyte, H. and Csorba, M., 2001. A solution to the simultaneous localization and map building (SLAM) problem. *IEEE Transactions on Robotics and Automation*, [online] Available at: <https://ieeexplore.ieee.org/document/938381 > [Accessed 4 January 2020].

48. Montemerlo, M., Thrun, S., Koller, D. and Wegbreit, B., 2002. FastSLAM: A Factored Solution to the Simultaneous Localization and Mapping Problem. *AAAI-02 Proceedings*, [online] Available at: <https://www.aaai.org/Papers/AAAI/2002/AAAI02-089.pdf > [Accessed 6 January 2020].

49. Bryson, M. and Sukkarieh, S., 2007. Building a Robust Implementation of Bearing-only Inertial SLAM for a UAV. *Journal of Field Robotics*, [online] Available at: <https://onlinelibrary.wiley.com/doi/abs/10.1002/rob.20178 > [Accessed 7 January 2020].

50. Schmuck, P. and Chli, M., 2017. Multi-UAV collaborative monocular SLAM. *IEEE*, [online] Available at: <https://ieeexplore.ieee.org/abstract/document/7989445 > [Accessed 9 January 2020].

51. Intel. 2020. *The Airborne Revolution In Drone Innovation*. [online] Available at: <http://www.asctec.de/en/uav-uas-drone-applications/uav-slam-simultaneous-localization-mapping/ > [Accessed 6 January 2020].

52. Nassi, B., Shabtai, A., Masuoka, R. and Elovici, Y., 2019. Security and Privacy in the Age of Drones: Threats, Challenges, Solution Mechanisms, and Scientific Gaps. [online] Available at: <https://arxiv.org/pdf/1903.05155.pdf > [Accessed 12 January 2020].

53. Nagai, M., Tianen Chen, Shibasaki, R., Kumagai, H. and Ahmed, A., 2009. UAV-Borne 3-D Mapping System by Multisensor Integration. *IEEE Transactions on Geoscience and Remote Sensing*, [online] Available at: <https://ieeexplore.ieee.org/abstract/document/4783021 > [Accessed 12 January 2020].

54. Kleiner, A., Prediger, J. and Nebel, B., 2007. RFID Technology-based Exploration and SLAM for Search And Rescue. *EEE*, [online] Available at: <https://ieeexplore.ieee.org/abstract/document/4059043 > [Accessed 10 January 2020].

55. Valencynetworks.com. 2019. *Network Security : Wifi Security Fixation | Pune Mumbai Hyderabad Delhi Bangalore India | Valency Networks*. [online] Available at: <https://www.valencynetworks.com/articles/cyber-attacks-wireless-attacks.html > [Accessed 15 November 2019].

56. Crawley, K., 2018. *Is Your Router Being Exploited By Cyber Attackers?*. [online] The Threat Report. Available at: <https://thethreatreport.com/is-your-router-being-exploited-by-cyber-attackers/ > [Accessed 11 November 2019].

57. Lupu, T., 2007. Main Types of Attacks in Wireless Sensor Networks. [online] Available at: <http://www.wseas.us/e-library/conferences/2009/budapest/MIV-SSIP/MIV-SSIP31.pdf > [Accessed 11 November 2019].

58. Weisman, S., 2019. *What Are Denial Of Service (Dos) Attacks? Dos Attacks Explained*. [online] Us.norton.com. Available at: <https://us.norton.com/internetsecurity-emerging-threats-dos-attacks-explained.html > [Accessed 13 November 2019].

59. Dedrone. 2018. *How Hackers Use Drones To Infiltrate Corporate Networks*. [online] Available at: <http://web-assets.dedrone.com/collateral/Dedrone-Cybersecurity-White-Paper.pdf > [Accessed 11 November 2019].

60. Buntz, B., 2017. *8 Drone-Related Security Dangers*. [online] IoT World Today. Available at: <https://www.iotworldtoday.com/2017/03/09/8-drone-related-security-dangers/ > [Accessed 10 November 2019].

61. Margaret Rouse. internet of things (IoT) (online) IoT agenta, . Available at:

<https://internetofthings agenda.techtarget.com/definition/Internet-of-Things-IoT> Accessed 11 November 2019].

62. Rouse, M., 2016. *What Is Iot (Internet Of Things) And How Does It Work?*. [online] IoT Agenda. Available at: <https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT > [Accessed 15 November 2019].

63. Econsultancy. 2019. *10 Examples Of The Internet Of Things In Healthcare – Econsultancy*. [online] Available at: <https://econsultancy.com/internet-of-things-healthcare/ > [Accessed 12 November 2019].

64. Travelers.com. 2019. *The Risks Of Iot In Medicine And Healthcare*. [online] Available at: <https://www.travelers.com/business-insights/industries/technology/the-risks-of-IoT-in-medicine-and-healthcare > [Accessed 10 November 2019].

65. Xiao-Feng, X. and Zun-Jing, W., 2016. Integrated In-Vehicle Decision Support System for Driving at Signalized Intersections: A Prototype of Smart IoT in Transportation. *Transportation Research Board 96th Annual Meeting*, [online] Available at: <https://trid.trb.org/view.aspx?id=1437314 > [Accessed 12 November 2019].

66. Boyes, H., Hallaq, B., Cunningham, J. and Watson, T., 2018. The industrial internet of things (IIoT): An analysis framework. *Computers in Industry*, [online] Available at: <https://www.sciencedirect.com/science/article/pii/S0166361517307285 > [Accessed 13 November 2019].

67. Hussain, S., 2018. *Quick Review Of Artificial Intelligence And Iot In The Aviation Industry*. [online] Medium. Available at: <https://medium.com/datadriveninvestor/quick-review-of-artificial-intelligence-and-iot-in-the-aviation-industry-15cfdccce060 > [Accessed 15 November 2019].

68. Statista Research Department. 2016. *Iot: Number Of Connected Devices Worldwide 2012-2025 | Statista*. [online] Available at: <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ > [Accessed 15 November 2019].

69. Hossain, M., Fotouhi, M. and Fotouhi, R., 2015. Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things. *2015 IEEE World Congress on Services*, [online] Available at: <https://ieeexplore.ieee.org/abstract/document/7196499/authors#authors > Accessed 17 November 2019].

70. Toms, L., 2016. *5 Common Cyber Attacks In The Iot*. [online] GlobalSign GMO Internet, Inc. Available at: <https://www.globalsign.com/en/blog/five-common-cyber-attacks-in-the-iot >

[Accessed 18 November 2019].

71. Hasan, M., 2019. *25 Most Common Iot Security Threats In An Increasingly Connected World*. [online] UbuntuPIT. Available at: <https://www.ubuntupit.com/25-most-common-iot-security-threats-in-an-increasingly-connected-world/ > [Accessed 17 November 2019].

72. Deogirikar, J. and Vidhate, A., 2017. Security Attacks inIoT: A Survey. *International conference on I-SMAC 2017*, [online] Available at: <http://faratarjome.ir/u/media/shopping_files/store-EN-1520245543-1185.pdf > [Accessed 2 December 2019].

73. Andrea, I., Chrysostomou, C. and Hadjichristofi, G., 2015. Internet of Things: Security vulnerabilities and challenges. *2015 IEEE Symposium on Computers and Communication*, [online] Available at: <https://www.researchgate.net/publication/304408245_Internet_of_Things_Security_vulnerabilities_and_challenges > [Accessed 2 December 2019].

74. Trendmicro.com. 2016. *Black Hat Demos Attacks On Iot, Bad Protocols, And Drones - Security News - Trend Micro USA*. [online] Available at: <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/black-hat-demos-attacks-on-iot-bad-protocols-and-drones > [Accessed 3 December 2019].

75. Barca, J. and Sekercioglu, Y., 2012. Swarm robotics reviewed. *Robotica*, [online] Available at: <https://pdfs.semanticscholar.org/105b/6ab10600bee3b4146c283490758281b7c98d.pdf >.

76. Intel. 2019. *Drone Light Shows Powered By Intel*. [online] Available at: <https://www.intel.com/content/www/us/en/technology-innovation/aerial-technology-light-show.html > [Accessed 4 December 2019].

77. Swarm-bots.org. 2005. *Swarm-Bots Project*. [online] Available at: <http://www.swarm-bots.org/> [Accessed 4 December 2019].

78. Gro, R., Bonani, M., Mondada, F. and Dorigo, M., 2006. Autonomous Self-Assembly in Swarm-Bots. *IEEE Transactions on Robotics*, [online] Available at: <http://www.swarm-bots.org/dllink.php@id=689&type=documents> [Accessed 4 December 2019]..

79. Raza, M., Iqbal, M., Sharif, M. and Haider, W., 2012. A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication. *World Applied Sciences Journal*, [online] 19. Available at: <https://www.researchgate.net/publication/236898951_A_Survey_of_Password_Attacks_and_Comparative_Analysis_on_Methods_for_Secure_Authentication> [Accessed 4 December 2019].

80. Ibm.com. 2020. *IBM Knowledge Center*. [online] Available at: <https://www.ibm.com/support/knowledgecenter/en/SSB2MG_4.6.0/com.ibm.ips.doc/concepts/wap_brute_force.htm> [Accessed 4 December 2019].

81. Basnet, R., Liu, Q. and Sung, A., 2012. Rule-Based Phishing Attack Detection. [online] Available at: <https://www.researchgate.net/publication/265919217_Rule-Based_Phishing_Attack_Detection/link/55b97c6b08aec0e5f43c35da/download> [Accessed 4 December 2019].

82. Kingsley-Hughes, A., 2008. *Elcomsoft Uses NVIDIA Gpus To Speed Up WPA/WPA2 Brute-Force Attack | Zdnet*. [online] ZDNet. Available at: <https://www.zdnet.com/article/elcomsoft-uses-nvidia-gpus-to-speed-up-wpawpa2-brute-force-attack/> [Accessed 8 December 2019].

83. Kwok, S. and Lam, E., 2008. Effective Uses of FPGAs for Brute-Force Attack on RC4 Ciphers. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, [online] Available at: <https://www.researchgate.net/publication/3338206_Effective_uses_of_FPGAs_for_brute-force_attack_on_RC4_ciphers> [Accessed 8 December 2019].

84. Aznar, F., Sempere, M., Pujol, M., Rizo, R. and Pujol, M., 2014. Modelling Oil-Spill Detection with Swarm Drones. *Abstract and Applied Analysis*, [online] 2014. Available at: <https://www.hindawi.com/journals/aaa/2014/949407/> [Accessed 8 December 2019].

85. Lamont, G., Slear, J. and Melendez, K., 2007. https://ieeexplore.ieee.org/abstract/document/4222976. *IEEE*, [online] Available at: <https://ieeexplore.ieee.org/abstract/document/4222976> [Accessed 8 December 2019].

86. Mail Online. 2011. *DIY Hacker Drone: Home-Made Surveillance Craft Can Launch Airborne Cyber Attacks*. [online] Available at: <https://www.dailymail.co.uk/sciencetech/article-2023732/DIY-hacker-drone-Home-surveillance-craft-launch-airborne-cyber-attacks.html> [Accessed 8 December 2019].

87. Greenberg, A., 2011. *Flying Drone Can Crack Wi-Fi Networks, Snoop On Cell Phones*. [online] Forbes. Available at: <https://www.forbes.com/sites/andygreenberg/2011/07/28/flying-drone-can-crack-wifi-networks-snoop-on-cell-phones/#59d371678564> [Accessed 9 December 2019].

88. Ezuma, M., Erden, F., Anjinappa, C., Ozdemir, O. and Guvenc, I., 2019. Micro-UAV Detection and Classification from RF Fingerprints Using Machine Learning Techniques. [online] Available at: <https://arxiv.org/pdf/1901.07703.pdf> [Accessed 9 December 2019].

89. Bom.gov.au. 2019. *How Radar Works*. [online] Available at: <http://www.bom.gov.au/australia/radar/about/what_is_radar.shtml> [Accessed 9 December 2019].

90. Molchanov, P., Harmanny, R., de Wit, J., Egiazarian, K. and Astola, J., 2014. Classification of small UAVs and birds by micro-Doppler signatures. *International Journal of Microwave and Wireless Technologies*, [online] Available at: <https://www.cambridge.org/core/journals/international-journal-of-microwave-and-wireless-technologies/article/classification-of-small-uavs-and-birds-by-microdoppler-signatures/C5A57FC02BBC4261CE563738ED9D6D76>[Accessed 9 December 2019].

91. Kim, J., Park, C., Ahn, J., Ko, Y., Park, J. and Gallagher, J., 2017. Real-time UAV sound detection and analysis system. *IEEE Sensors Applications Symposium (SAS)*, [online] Available at: <https://ieeexplore.ieee.org/abstract/document/7894058> [Accessed 16 December 2019].

92. E. E. Case, A. M. Zelnio and B. D. Rigling, "Low-Cost Acoustic Array for Small UAV Detection and Tracking," *2008 IEEE National Aerospace and Electronics Conference*, [online] Available at: <https://ieeexplore.ieee.org/abstract/document/4806528 > [Accessed 16 December 2019].

93. Gökçe, F., Üçoluk, G., Şahin, E. and Kalkan, S., 2015. Vision-Based Detection and Distance Estimation of Micro Unmanned Aerial Vehicles. *Sensors*, [online] 15. Available at: <https://www.mdpi.com/1424-8220/15/9/23805>[Accessed 16 December 2019].

94. Subcommittee on Oversight and Management Efficiency of the House Committee on Homeland Security, 2015. *Statement On The Security Threat Posed By Unmanned Aerial Systems And Possible Countermeasures*. [online] Austin: University of Texas. Available at: <https://radionavlab.ae.utexas.edu/images/stories/files/papers/statement-humphreys-20150318.pdf> [Accessed 16 December 2019].

95. Heliguy.com. 2017. *Geofencing And Drones - What You Need To Know*. [online] Available at: <https://www.heliguy.com/blog/2017/02/16/heliguys-guide-to-geofencing/> [Accessed 16 December 2019].

96. Whitefox Defense Technologies, Inc., 2018. *How To Evaluate Counter-Drone Products*. [online] Available at: <https://uploads-ssl.webflow.com/57e49943d82fa82e4e4491b4/5b440bfdfcf477c2b1ee9d89_WF-CounterDrone-WhitePaper-180709.pdf> [Accessed 16 December 2019].

97. Liberatore, S., 2015. *Crime Fighting Drones In Japan Are Keeping Public Officials Safe*. [online] Mail Online. Available at: <https://www.dailymail.co.uk/sciencetech/article-3356746/How-catch-drone-BIGGER-drone-giant-net-Tokyo-police-reveal-bizarre-UAV-catcher.html> [Accessed 16 December 2019].

98. Williams, R., 2015. *Tokyo Police Are Using Drones With Nets To Catch Other Drones*. [online] The Telegraph. Available at: <https://www.telegraph.co.uk/technology/2016/01/21/tokyo-police-are-using-drones-with-nets-to-catch-other-drones/> [Accessed 17 December 2019].

99. Mogg, T., 2018. *This Net-Blasting Security Drone Can Stay Airborne Forever. Here'S How.*. [online] Digitaltrends.com. Available at: <https://www.digitaltrends.com/cool-tech/dronecatcher-upgrade-hover-around-the-clock/> [Accessed 17 December 2019].

100. Airports Traffic International, 2018. *Annual World Airport Traffic Report*. Annual World Airport Traffic Forecasts 2018– 2040. [online] Available at: <https://aci.aero/wp-content/uploads/2018/11/WATR_WATF_Infographic_Web.pdf> [Accessed 22 December 2019].

101. Cisco Internet Business Solutions Group (IBSG), 2009. *Smart Airports: Transforming Passenger Experience To Thrive In The New Economy*. [online] Available at: <https://www.cisco.com/c/dam/en_us/about/ac79/docs/pov/Passenger_Exp_POV_0720aFINAL.pdf> [Accessed 22 December 2019].

102. Upadhya, V. and Rawat, D., 2014. *Intelligent Airports - Your Runway To Success*. [online] Wipro. Available at: <https://www.wipro.com/content/dam/nexus/en/industries/engineering-and-construction/latest-thinking/2401_intelligent-airports-your-runway-to-success.pdf> [Accessed 22 December 2019].

103. Voulgaris, C. and Karampelas, A., 2018. Smart Airport Athens International Airport "Eleftherios Venizelos" Case. [online] Available at: <https://hellanicus.lib.aegean.gr/bitstream/handle/11610/18806/Thesis_Smart_Airport.pdf?sequence=1> [Accessed 22 December 2019].

104. Delain, O., Ruhlmann, O. and Vautier, E., 2016. *Cyber-Security Application For SESAR OFA 05.01.01 - Final Report*. [online] Helios. Available at: <https://www.sesarju.eu/sites/default/files/documents/news/Addressing_airport_cyber-security_Full_0.pdf> [Accessed 22 December 2019].

105. Lykou, G., Anagnostopoulou, A. and Gritzalis, D., 2018. Smart Airport Cybersecurity: Threat Mitigation and Cyber Resilience Controls. *Sensors*, [online] 19. Available at: <https://www.mdpi.com/1424-8220/19/1/19>[Accessed 22 December 2019].

106. Federal Aviation Administration, 2019. *FAA Aerospace Forecast 2019-2039*. [online] Available at: <https://www.faa.gov/data_research/aviation/aerospace_forecasts/media/FY2019-39_FAA_Aerospace_Forecast.pdf> [Accessed 23 December 2019].

107. Homeland Security Investigations SAC Intelligence Program Los Angeles, 2017. *(U) Da Jiang Innovations (DJI) Likely Providing U.S. Critical Infrastructure And Law Enforcement Data To Chinese Government*. [online] US Immigration and Customs Enforcement. Available at: <https://info.publicintelligence.net/ICE-DJI-China.pdf> [Accessed 23 December 2019].

108. Mozur, P., 2016. *China Drone Maker Says It May Share Data With State*. [online] Nytimes.com. Available at: <https://www.nytimes.com/2016/04/21/world/asia/dji-drones-

china.html> [Accessed 27 December 2019].

109. Zetter, K., 2014. *DIY Spy Drone Sniffs Wi-Fi, Intercepts Phone Calls*. [online] WIRED. Available at: <https://www.wired.com/2011/08/blackhat-drone/> [Accessed 27 December 2019].

110. Jones, J., 2010. *Over 40 Publications / Studies Combined: UAS / UAV / Drone Swarm Technology Research*. https://books.google.gr/books?id=2U9LDwAAQBAJ&dq=UAS+and+espionage&hl=el&source=gbs_navlinks_s [Accessed 27 December 2019].

111. Margaritoff, M., 2018. *Watch A Drone Crash Onto Apple Park Campus' 'No Drone Zone'*. [online] thedrive.com. Available at: <https://www.thedrive.com/article/18609/watch-a-drone-crash-onto-apple-park-campus-no-drone-zone> [Accessed 27 December 2019].

112. Guri, M., Zadov, B., Atias, E. and Elovici, Y., 2017. LED-it-GO Leaking (a lot of) Data from Air-Gapped Computers via the (small) Hard Drive LED. [online] Available at: <https://arxiv.org/ftp/arxiv/papers/1702/1702.06715.pdf> [Accessed 29 December 2019].

113. Reade, L., 1958. *Bombs Over Venice | History Today*. [online] Historytoday.com. Available at: <https://www.historytoday.com/archive/bombs-over-venice> [Accessed 29 December 2019].