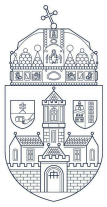

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORAL (PH.D.) THESIS BOOKLET

MAHMOD AL-BKREE

UNMANNED AERIAL SYSTEMS APPLIED TO SOLVE SAFETY AND SECURITY PROBLEMS

Scientific Supervisor
Prof. Dr. habil. Róbert Szabolcsi

DOCTORAL SCHOOL ON SAFETY AND SECURITY SCIENCES

09 October 2024

Contents

Summary

The need for reliable security solutions in facilities with sensitive perimeters, such as critical infrastructure, residential areas, and international borders, has prompted the search for innovative solutions that can cover more areas while being affordable. Traditional security systems face challenges in terms of efficiency, reliability, and cost-effectiveness when dealing with large dimensions, which is cost-prohibitive. The aim of this thesis is to explore the use of Unmanned Aerial Vehicles (UAVs) to address the security concerns associated with large outdoor perimeters to develop a methodology that maximises the benefits of UAVs. The research plan focuses on the design of a comprehensive UAV system that enhances efficiency, reliability, and cost-effectiveness, with a specific emphasis on image processing. The proposed UAV system combines modern methods and principles to achieve the primary goal of reconnaissance, providing real-time information and periodic surveillance data, and optimising the 5Ds – Demarcation, Deterrence, Detection, Delay, and Defeat of intruders.

In this research, we have identified the potential threat spaces and proposed a UAV system that collects data on a regular basis (e.g. one sortie per day), and is designed for the minimum viable requirements of cyber-physical security measures, sensors, and data processing algorithms using tools such as image registration to electronically filter out extraneous data. This proposal is expected to minimise the number of surveillance sorties by successfully detecting intrusion clues and reducing the manpower required for image analysis by computerising the process; as well as reducing the data storage to a fraction of the amount collected. Although UAVs have been used for border surveillance for decades, confidentiality and privacy issues have limited the publication of their operational data, preventing a significant number of practical results from being researched. Another challenge is to find the interoperability relationship between sensors to identify which combination of sensors has the highest probability of detecting certain clues, ultimately improving the system efficiency, and the successful handling of the collected data.

We have investigated how a well-designed UAV surveillance system, using advanced sensors, could enhance current perimeter security measures, how periodic surveillance over large areas could significantly reduce costs, and how the data collected from a periodic surveillance could be as valuable as other means of surveillance from a cost/value perspective.

1. Background Of The Research

Currently, the security concerns about protecting the perimeters of large facilities have encouraged many scholars to tackle the topic from different points of view [1]. Critical infrastructures, residential areas, and international borders require a security system that applies multidisciplinary research and has maximum preventive feedback. In this chapter, I summarise the state of the art contribution by reviewing the most relevant scientific literature.

The adoption of a total mostly automated border surveillance strategy yields multifaceted benefits by deterring potential intruders [2]. Enhanced situational awareness enables proactive responses to potential threats, preventing illegal activities and safeguarding human and economic interests. In addition, the systematic collection of data facilitates evidence-based policy making. Many policymakers are pushing for accomplishing more surveillance on the borders [3], resource allocation, and the continuous improvement of surveillance methodologies for the future humanity dreamed of for safety, prosperity, and happiness [4]. Smart border surveillance represents a holistic and forward-looking approach to securing critical frontiers. By embracing advanced technologies, fostering collaboration such as UAVs, and leveraging intelligence, countries can fortify their borders against a spectrum of threats [5]. As the global landscape continues to evolve, the need for intelligent border surveillance remains critical to ensuring the integrity and security of critical infrastructure. In Europe, Eurosur is designed as a system that gathers surveillance data from different units and technologies into a single centre and produces situational awareness of the borders [6] & [7]. It is used in "monitoring, detection, identification, tracking, prevention, and interception of unauthorised border crossings" [8].

To ensure higher security measures, border protection agents usually utilise multiple advanced technologies such as biometric sensors, unattended ground-based thermal imagers, UAV systems, radiation detectors, surveillance equipment, radiation isotope identification devices, vehicle and cargo inspection systems, integrated fixed observation towers, X-ray and Z backscatter technology which produce photo-like images that help reveal most organic threats and contraband for the detection of drugs, currency, explosives, and plastic weapons [9].

Figure 1. illustrates some of the technologies used for border protection, these technologies are usually focused on higher-risk areas and near the populated regions, for remote areas periodic surveillance patrols are chosen for affordability, sign-cutting and tracking, UAV overflights, and partnership with communities are examples of programmes and techniques

that might be chosen for specific areas [9]. Border surveillance UAVs were used in anti-drug smuggling operations on the United States-Mexico border in Texas by the Marines piloting it for weeks in February 1990. The operation originally intended to counter drug smuggling resulted in the detection of hundreds of illegal crossings and apprehensions [10]. UAVs have been used for different types of transnational criminal activity, including by drug traffickers to transport drugs across security zones, weaponized UAVs have also been reported, in the years 2012, 2013, and 2014, around 150 criminal drone incursions were documented by the US Drug Enforcement Administration [11].

Figure 1. Illustration of border protection technologies [9]

To minimise the losses caused by infringement on perimeters we need a standardised measurement that can be used to evaluate solutions, while any life loss is a priceless tragedy, and any inconvenience is a resounding defeat, estimating the losses in financial terms is still practised for the practicality of research. In [12] they have reported that “Transnational crime will continue to grow until the paradigm of high profits and low risk is challenged. This report calls on governments, experts, the private sector, and civil society groups to seek to address the global shadow financial system by promoting greater financial transparency”, Table 1. shows the estimated annual value of different transnational crimes.

Transnational Crime	Estimated Annual Value (US$)
Drug Trafficking	$426 billion to $652 billion
Small Arms & Light Weapons Trafficking	$1.7 billion to $3.5 billion
Human Trafficking	$150.2 billion
Organ Trafficking	$840 million to $1.7 billion
Trafficking in Cultural Property	$1.2 billion to $1.6 billion
Counterfeiting	$923 billion to $1.13 trillion
Illegal Wildlife Trade	$5 billion to $23 billion
IUU Fishing	$15.5 billion to $36.4 billion
Illegal Logging	$52 billion to $157 billion
Illegal Mining	$12 billion to $48 billion
Crude Oil Theft	$5.2 billion to $11.9 billion
Total	**$1.6 trillion to $2.2 trillion**

Table 1. The estimated annual value of different transnational crimes (Source: [12])

On the other hand the cost of security measures starting with human resources, not only in terms of salaries but also in terms of risk and the emotional costs is staggering, according to [13], the cost of stress, anxiety, depression, and related psychological and physical effects costs $125-$190 billion per year in the US, those emotional costs are highest among the employees of the security sector.

The cost of perimeter security constitutes a significant aspect of any comprehensive security strategy, and preventive measures to encompass various elements essential for safeguarding physical boundaries. The investment per kilometre can vary significantly depending on a number of factors such as the type of technology used, geographical terrain, existing infrastructure, and specific security requirements, so flexibility in system design is required. In general, estimates range a wide range, from tens of thousands to millions of dollars per kilometre, depending on the complexity and sophistication of the surveillance system. [14] explores “how border practices between states resonate with bordering practices between the human and non-human” which requires the system to define what it is trying to detect when it comes to non-humans beings, as well as objects.

Basic measures such as fencing and low-tech surveillance can be at the lower end of the spectrum [15], while advanced technologies such as high-tech sensors, UAVs, and integrated monitoring systems can increase costs significantly. In addition, factors such as accessibility, environmental conditions, and the need for ongoing maintenance can contribute to the overall cost. The common denominator in reducing costs is computerization as the computing power continually increases functionality and reduces the resources needed. [16] have quoted a

statement about a “recent legislative proposals would have mandated that the US Border Patrol accomplish 100% ‘‘persistent surveillance’’ and an ‘‘effectiveness rate’’ of 90% (to be calculated by dividing the total number of unauthorised incursions detected in a given area by the total number of apprehensions or ‘‘turn backs’’) along all US land borders”.

Unmanned Aerial Vehicles (UAVs), commonly known as drones, have emerged as indispensable tools for border surveillance, offering diverse capabilities to enhance monitoring and security [17]. The dynamic landscape of border challenges requires a variety of UAVs, each designed to meet specific requirements and operational environments [10]. In [18] a main and robust framework for the UAS was given, describing its main parts with further analysis.

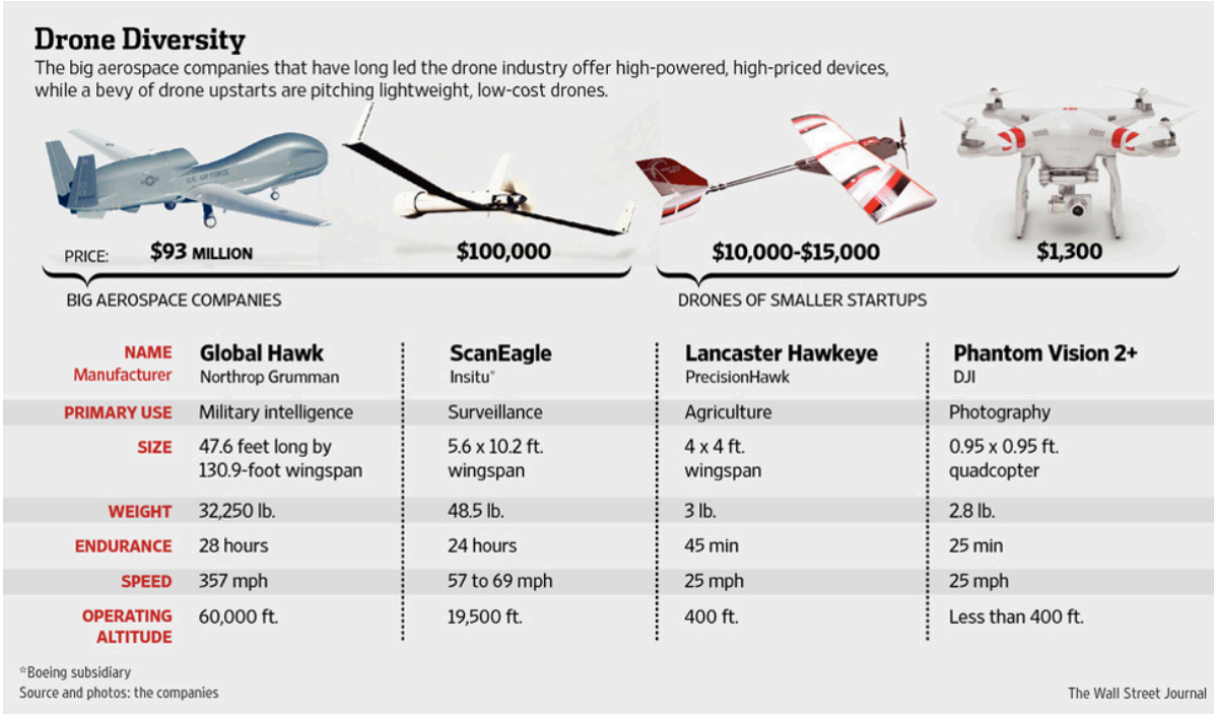

Figure 2. UAV Diversity [19]

the research reviewed on perimeter surveillance, which addresses several conceptual issues related to the dimensionality of border vulnerabilities. The works explore recent strategies and technologies aimed at enhancing security, as well as the costs associated with both criminal activities and their countermeasures. Additionally, they delve into psychoanalytic theories and the commonplace nature of border surveillance, demonstrating the effectiveness of various technologies while also highlighting implementation errors linked to existing policies, regulations, and public perceptions. The analysis converges on identifying key factors that may influence perimeter security challenges over the next 15 years, illustrating that perimeter

security phenomena are intertwined with numerous accelerating multivariate dynamics. This necessitates that administrators adopt multi-level measures to manage or restrict access to individuals, objects, and information. In this research, I have selected a few factors based on,

1. The impact on global security in the years 2020-2035
2. The impact on automation/computerization.
3. The impact on other fields.
4. The adaptability to new situations, conditions, or circumstances.

2. Objectives

This Ph.D. thesis aims to contribute to the field of perimeter security technology by investigating the design and implementation of a UAV system tailored for large perimeter facilities where a set of sensors can fly periodically to collect data along the target area. The research objectives are to design a UAV system using modern methods and principles. The envisioned system targets the fundamental goal of surveillance, providing information crucial for securing extensive perimeters and optimising the 5Ds of security – Demarcation, Deterrence, Detection, Delay, and Defeat.

3. Research Methods

Investigated in this research is the design for cyber-physical security, as preventive measures to secure the UAV system itself from getting attacked on the information level by allowing criminals access to diagnostic capabilities and strategies, therefore operating “under the radar” rendering the system ineffective. And physical level where secured areas could be breached by people or objects, sabotaging material, equipment, or infrastructure. Identification of six main threat spaces to the system, and showing the steps of minimising these threats starting from the supply chain of the system components and selecting the suitable antenna, conducting periodic network mapping, also implementing multiple positioning techniques strengthening the navigation system immunity to spoofing, as well as selecting an encryption that balances the security and system resources needs.

The second factor is big data processing. In the literature, the electronic detection of objects in aerial video and tracking moving objects have been successfully demonstrated, which significantly improved UAV surveillance. In the forthcoming chapters, I will present my

findings on the importance of computerising the sign-cutting process. I propose an image registration technique designed to electronically detect sign-cutting clues in periodic surveillance images. In case the preventive layer of the perimeter fails to stop intruders, sign-cutting would help to detect the clues even after a potential breach has occurred.

The fourth factor is design for adaptability, the variety of perimeter security needs, and the constant changes in situations, conditions, or circumstances impede a “one solution fits all” approach. I have proposed a design to be adaptable to the uncertainties of perimeter requirements (length, height, technologies…). but based on a risk assessment evaluate the cost/benefits ratio of each component by creating an unlimited dimensional selection criteria.. The foundation would be to regularly assess the available resources and the future multiple emerging technologies and techniques to help determine what data to collect, and how to collect. When and where, this will allow decision makers to design a system based on the available budget, or based on the efficiency level, or based on expected future innovations, starting with a pilot trial that is scalable to fit higher needs, the models optimise the technology selection and the distribution along a perimeter.

4. Managing The Cyber-Physical Security Of The System

The majority of cyber threats to the UAV come through its antennas (onboard wireless transceivers) during flight, the antenna is the main physical port for cybersecurity attack vectors, threats either by sending a hacking code through it, or by receiving sensitive data transmitted by the antenna to the GCS, or by jamming it, prohibiting it from communicating at all.

Limiting the propagation beam of the data link between the GCS and the UAV to a narrow space can protect from these threats, and strengthen the antenna’s gain, improving the signal range and minimising the Freshnel zone radius. Using phased array antennas for the UAV, GCS, or both can create a safer line of communication, reducing the exposed space of attack to an order of magnitude.

When the data is transmitted omnidirectionally it creates a spherical propagation that allows an attacker to receive the data from any point in that sphere while focusing the transmission direction into a very limited cone of space minimises the attacker’s chances of receiving the signal outside, attacks such as the man in the middle (MITM), Denial of Service (DoS), and data capture are examples of omnidirectional antenna vulnerabilities.

An automated vulnerability scanner can highlight most of the critical attack points in the network [20], with a detailed description of the cyber problem, comparable to the Common Vulnerabilities and Exposures (CVE), and suggest a variety of possible solutions and advisories to secure them.

Knowing the characteristics of the network, all (used & unused) devices, hosts, ports, hops, operating systems, services, and applications is essential for managing its security, therefore, regular scanning of the network to ensure that the hardware and software connected is benign and adequately secure would reduce the risk of attack. Scanning is the main tool that an attacker would use to find vulnerabilities, incidents of attackers getting access to the UAV controller, WiFi connection, and GCS computers have been reported. Identifying the ports and their functions will help to eliminate the unnecessary ones and adequately secure the rest of them.

Lack of adequate encryption is one of the most common vulnerabilities, Wi-Fi Protected Access® (WPA) is a common data encryption for wireless networks and can establish secure wireless communication between the UAV and the GCS, the third version WPA3 could use 128-256 bit session key size with simultaneous authentication, it uses the Advanced Encryption Standard (AES) method which from an encryption point of view is sufficient for adequate security and is widely used in modern UAVs, however, for an onboard UAV the processing power and memory may in some cases require a lighter encryption method such as Bleep64 which is a small, fast, and effective, consuming much less processing power and memory, and does not require special encryption hardware [R1].

The large amount of cybersecurity data and its complexity is beyond the manual ability of humans to organise and act on, however, Machine Learning (ML) models thrive on big data. The use of ML could classify suspicious network activity and predict some threats changing the reactive nature of cybersecurity and assisting the available human resources.

Onboard the UAV machine learning models could instantly identify potential threats, with models such as motion and event detection having high accuracy to provide early warning of suspicious activity. For surveillance UAVs where the perimeter is large, the area will be under periodically interrupted surveillance, leaving segments of the protected area unsurveilled for an extended amount of time, using a machine analytics model for man-tracking and sign-cutting would help in terms of acquiring information about previous events, and it can identify if suspicious electronic devices have been planted near the perimeter, by comparing

the current video stream with the stream from the previous days and highlight the differences in the two videos.

One of the most cost-effective performance techniques is to compare the Doppler residual resulting from the relative motion of the satellites and the UAV, producing a spoofed signal that matches the Doppler residual of the legitimate signal is relatively complex. Detecting the spoofed signal is normally effective at rejecting their data, however, it has a low chance of isolating the legitimate data for correct positioning. The consequences for failing to receive legitimate GPS data by analysing the signals can be mitigated by integrating other positioning methods suggested including the following,

1. Positioning Based on Inertial Measurement Unit IMU
2. Local Positioning System LPS
3. Positioning Based on Vision and Other Sensors

5. Sign Cutting And Image Registration

Man-tracking and sign cutting are some of the most essential tools to analyse surveillance footage as they provide clues about events that have happened during the surveillance absence. However, it's highly recommended to automate the manual process that consumes a lot of time and manpower. The recent advances in Unmanned Aerial Vehicles (UAVs), Camera resolution, and most importantly computer vision & visual recognition technology make the argument to computerise the Man-tracking process so compelling. In this research, we investigate the possibilities and limitations of computer vision in this field. It's important to highlight here that our focus is on past events tracking, detecting signs 1-24 hours old, not the ground moving target tracking where the computer vision detects a moving object and follows it in real-time.

Physical signs could be vehicle or footprints, soil disturbances, broken branches, bruised vegetation, recent campfires, leftover objects, and any changes to the environment. Detecting these signs could increase the effectiveness of surveillance. These clues are detected by object detection algorithms that use machine learning and deep learning architectures to analyse image data and recognise objects working on the principles of convolutional neural networks, Region-Based Convolutional Neural Networks (R-CNN), Fast R-CNN and You Only Look Once (YOLO) with recognition efficiency of around 80-90%, or by human aided by image

registration algorithm that highlights the existence of the new changes in the UAV surveillance path.

In some instances objects could be left behind either by trashing them or intentionally planting them in the vicinity to collect data, the target would be detecting the object itself or its effects e.g. electromagnetic signals could be searched for. Atmospheric variations are the main contributor to a high signal-to-noise ratio, as the various intensities of sunlight, clouds, and seasons require a large versatile dataset to train the neural network on, the image can be divided into smaller images in case of a large body of water is visible in the frame, the sky and clouds have similar effect. Shadows usually create smaller differences than real objects.

The scanning mission starts by flying the initial predetermined surveillance path, collecting image data from the defined parameters of altitude, lens angle, and zoom, the automatic image registration detects the number of changes per frame and the percentage of that change and calculates the total weight of that change, based on a predetermined threshold, the algorithm could call for a human supervisor action or continue the scan, the collected data is used for self-learning of the algorithm, illustrated in Figure 3.

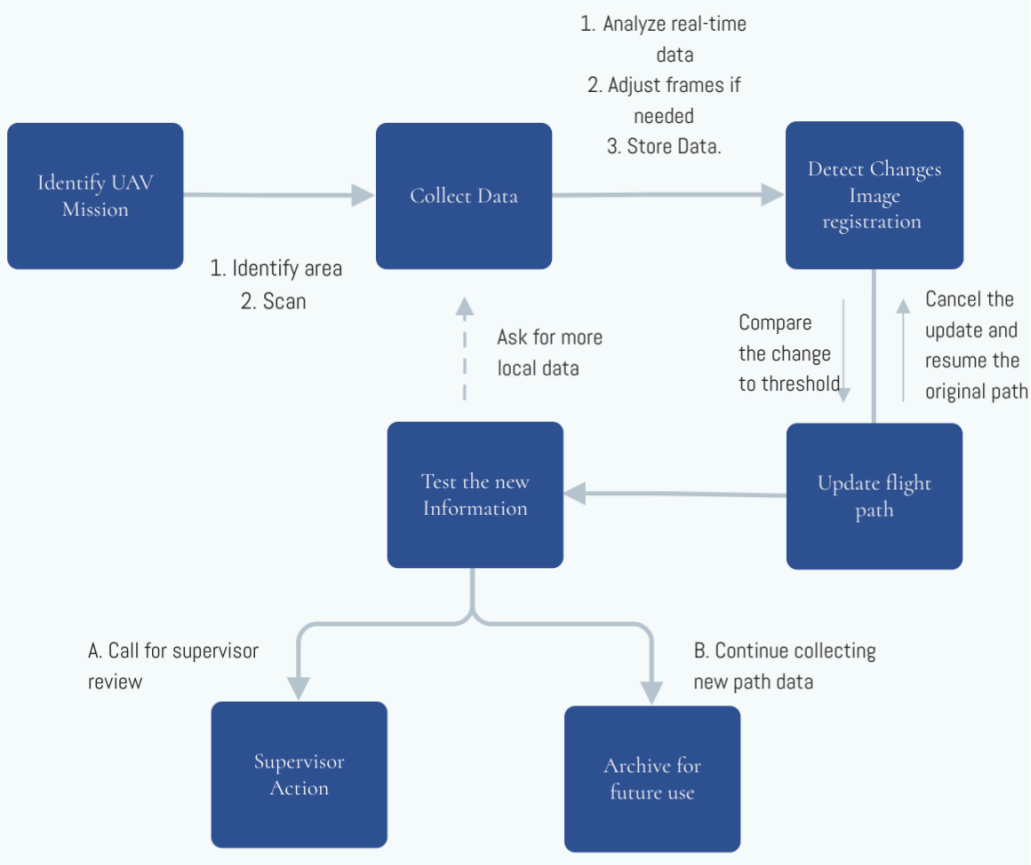

Figure 3. Flowchart illustration of a scanning mission [Author]

Image registration is the procedure where two or more images of the same field are aligned together using markers, it's widely used in the medical field diagnostic tests such as magnetic resonance imaging that collects 3D data of living organs to monitor changes inside the organ tissues. It's also a common procedure in analysing satellite imagery, in our case the first imagery taken to the certain region are the baseline to compare with the future imagery of the same region, if the field view angle is not completely the same, a geometric displacement is necessary to realign them together, changing the UAV position, camera, the scene lighting, or any element in the scene will result in a change in the alignment of that image group [R4].

Computerising the process of image analysis is solving the overwhelming size of surveillance imagery collected daily, one approach would be dividing the surveilled area into smaller pieces that fit the UAV camera frame, selecting the same spatial position to capture the image to ensure the maximum possible overlapping between the two images which will ultimately reduce the signal-to-noise ratio (SNR). For the same area, images from multiple angles and altitudes could be taken. The repeatability of the UAV positioning is important to increase the overall quality of the process although there are many techniques to compensate and automatically realign the two images all of them would affect the final efficiency.

The algorithm assumes the same-size image feed for every iteration, and to reduce the effect of different brightness and contrast, a multimodal intensity registration has been used. To evaluate the accuracy of the registration the mean squared error was selected, and the optimisation of the overall alignment feedback is done by phase correlation for the initial images. The final judgement of registration result quality was evaluated subjectively case by case as some signs need emphasis on the intensity, while other cases might need more emphasis on the misalignment between the two images. So far, I could not find one universal metric to quantify the overall quality of detection. In all cases, manual fine-tuning of parameters gave slightly better results, however, for this research only automated setup was considered. All trials performed on stable images taken minutes apart to prove the concept, longer gaps are likely to be more challenging, especially in terms of false positive alarms from detecting noise.

The misregistration caused by the different brightness can be in many regions of the image, the algorithm can be set to contour the N segments of the image that have the highest intensity difference. An example of a surveillance sign detected by the model. Figure 4. shows a sign of a previous activity detected by a machine learning model, which will instigate a further investigation, and could update the UAV mission to focus on the area looking for more signs.

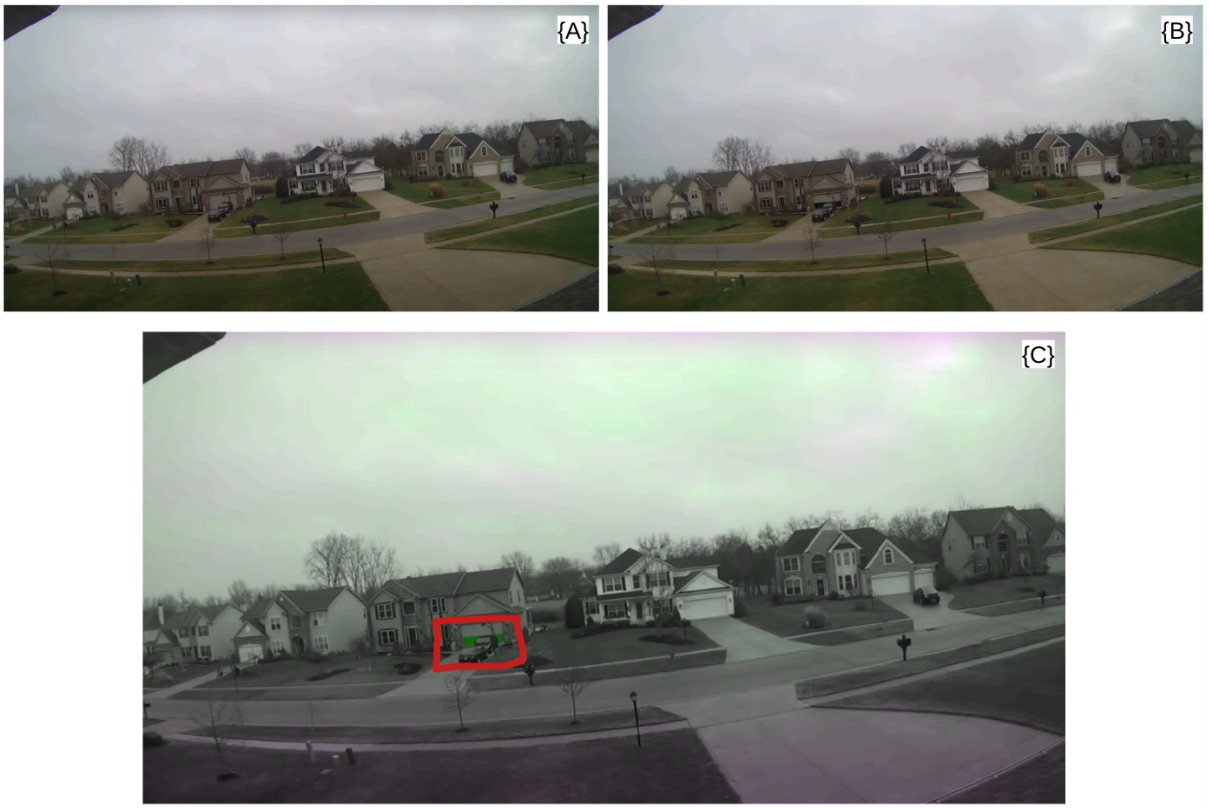

Figure 4. A. Shows the first surveilled scene, B. shows the location after time interruption, C. shows the detected sign (A & B were sourced from [21], C is processed by Author).

6. Case Study Of A Proposed Solution: Example Of Jordan

I used the example of Jordan as a case study for the proposed solution. Jordan is an Arab country in Southwest Asia located between N. Latitude 29° 11' and 33° 22' and E. Longitude 34° 59' and 39° 12'. It is bordered by Syria to the north, Iraq to the east, Saudi Arabia to the east and south, and Palestine to the west, and the country is in a continuous effort to stop smuggling activities on the border that include drugs, weapons, and foreign fighters. Iraq shares 181 kilometres of international border with Jordan, Syria 375 kilometres, Palestine 335 kilometres, 26 kilometres of coastline, and Saudi Arabia 728 kilometres, adding to 1,645 kilometres of total border length.

The system is based on adding the element of UAV surveillance to increase the level of protection of the border against various threats, each technology will be given a value based on the threat assessments in terms of severity and probability of occurrence, the history of intrusions along the certain segment of the border as well as the natural condition of the different terrains will influence the effectiveness of the countermeasure, therefore, based on

the operational value of each technology and its cost the model would prioritise their selection. The evaluation sequence is as follows,

1. Identify which border segment needs surveillance;
2. Identify the potential threats for that segment;
3. Analyse the appropriate surveillance technology to detect the threats;
4. Assign a benefit value to the technology and the cost of acquiring it.

To select among tens of different technologies used in security drones a comparative assessment of their overall cost-benefit ratio is needed. While one technology may vary greatly in terms of quality, or performance, the assessment is useful as a baseline for selection that can be overvoted by the decision-maker whenever a valid need arises in a particular application context. The rating is based on ten criteria, (data criticality, data quantity, data integrity, human support, ease of use). Camera data (video and still images) is the most widely used sensor for border security as it captures a high amount of critical data, it's reliable and relatively easy to use, the competition for UAV cameras are satellite cameras, manned aircraft cameras, or fixed & mobile ground cameras in specific areas of the border, the trade-off benefits of UAV cameras are the mobility, cost, ability to operate unobtrusively, and cover a massive area.

To optimise the distribution of the UAV bases an Integer Linear Programming (ILP) model can be used, and another ILP model is used to optimise the technologies selection as follows,

ILP Model A.

The Kingdom of Jordan's air bases are King Abdullah Air Base at Marka which is right on the edge of the capital governorate of Amman, King Hussein Air Base at Al Mafraq Governorate just a few kilometres to the northeast of Mafraq city, and Prince Hassan Air Base at pumping station H5 in the desert of Safawi 75 kilometres northeast of Amman. Muwaffaq Salti Air Base at Azraq in the eastern desert, and King Faisal Air Base at Al Jafr in the southern desert, as shown in Figure 43. The ground bases for the UAVs would be selected based on the security demand along the border, the allocated budget, and the proximity of existing force stations and patrols [R2].

Figure 43. Map of the Royal Jordanian Air Force bases distribution [22]

The first, discrete optimisation model, the maximum coverage formulation, is based on 10 potential base locations near the border, to find the minimum number of ground bases that can cover the selected segment of the border. Starting from Irbid city as an area 1 in the northwest and flying counter-clockwise along the border up until Ramtha city as area 10, the border is divided into segments each has a length of 200 kilometres, with a 35 kilometres of overlap between every two segments represented as x1, x2, ...x10, the UAV flight range is 600 kilometre so the UAV can bypass at least one ground base at a time whenever needed.

The objective function is:

Minimise $\sum x_j$, j (j from 1 to 10)

Set of constraint

$$
\begin{aligned}
x_{10} + x_1 + x_2 &\geq 1 \quad \text{(area 1)} \\
x_1 + x_2 &\geq 1 \quad \text{(area 2)} \\
x_2 + x_3 + x_4 &\geq 1 \quad \text{(area 3)} \\
x_3 + x_4 &\geq 1 \quad \text{(area 4)} \\
x_4 + x_5 + x_6 &\geq 1 \quad \text{(area 5)} \\
x_5 + x_6 &\geq 1 \quad \text{(area 6)} \\
x_6 + x_7 &\geq 1 \quad \text{(area 7)} \\
x_6 + x_7 + x_8 &\geq 1 \quad \text{(area 8)} \\
x_8 + x_9 &\geq 1 \quad \text{(area 9)} \\
x_9 + x_{10} + x_1 &\geq 1 \quad \text{(area 10)} \\
(x_1, \ldots, x_{10}) &\text{ are binary.}
\end{aligned}
$$

ILP Model B.

A knapsack model is proposed to optimise the number of sensors to be carried on each UAV, as the same vehicle can cover the whole border, it will have at least 2 bases to land for maintenance and refuelling, no one technology can be selected (n+1) independent times unless all other needed technologies got selected for at least (n) times. The following Table 6. shows the technology costs and operational values for the Camera, Lidar, Physical/Biological Samples Collectors (PBSC), Hyperspectral Camera, Radar, Tele-Communication Human to Machine means (TCHM), Object Installer Capability (OIC).

	Camera	Lidar	PBSC	Spectral Camera	Radar	TCHM	OIC
Cost (thousands)	1	20	28	15	1	5	40
Value	100	60	55	90	90	70	100

Table 2. Samples of technology costs and operational values [Author]

Given a budget of $80,000, the following model is used to maximise the values/cost. Yj represents technology (1 if selected, 0 otherwise).

The objective function is:

$$\text{maximize} \quad 100x_1 + 60x_2 + 55x_3 + 90x_4 + 90x_5 + 70x_6 + 100x_7$$

Set of constraints:

$$x_1 + 20x_2 + 28x_3 + 15x_4 + 1x_5 + 5x_6 + 40x_7 \leq 80$$

Results of Models A & B,

Applying the above models shows that at least 4 ground bases are needed to cover the length of the border (x2, x4, x6 and x9). Technology-wise running the model result of selecting (4 cameras, 3 radars, 2 TCHM, 1 spectral camera, and 1 Lidar). However, from a practical view, the result in this case shows repetitive selection of the same technology reducing the overall operational value, while other technologies did not get selected at all due to budget limitations. An additional $2000 to the budget would result in getting six different technologies (all except PBSC). The metric for estimating the operational value is a dynamic multi-dimensional equation that considers the repetitiveness of selecting a technology, also provides insight into the budget brackets, and most importantly modulates the interoperationility of multi-sensory data. Table 7. was used to evaluate the operational value of different sensor systems.

7. New Scientific Results

The essence and meaning of my scientific research work made during my Ph.D. studies can be summarised in the following theses:

Thesis No1

The cost-prohibitive persistent surveillance can be optimised into a periodic surveillance system that significantly reduces the number of sorties, while still providing valuable data. [R2] and [R4].

Thesis No2

An industry-standard level of safety can be achieved, for the system’s additional potential threats. I identified six methods of increasing the system's immunity while maintaining the overall cost advantage, and showed that the high rate of crashes is largely due to the new designs, or underinvestment by choosing compromised technologies. I found no evidence that non-compact manned surveillance vehicles are significantly safer than UAVs. [R1].

Thesis No3

Using an automated image registration technique, the successful detection of clues that aid in automating the process of sign-cutting is achieved. [R1] and [R4].

8. Conclusion

This research highlights the urgent need for additional security measures to safeguard the extensive perimeters of critical infrastructure. It investigates the use of UAV systems equipped with advanced sensors to minimise potential threats by gathering and processing surveillance data. The focus is on three main objectives: identifying the current capabilities for collecting quality data; determining what needs to be added, such as automating the filtering and analysis processes; and validating these needs through the application of technologies, techniques, and strategies in designing a case study. My research findings indicate that UAV systems cannot be replaced by alternative systems to increase efficiency, and that periodic surveillance can provide valuable information.

Jordan currently uses physical barriers of walls and fences on some segments of the border, in addition to regular security personnel patrolling areas near the border, as well as multiple layers of technologies including cameras and radars with variant bands of the spectrum, buried in the ground seismic and acoustic sensors, both permanent fixed and mobile sensors carried on ground and aerial vehicles. The design of border surveillance is virtually identical to looking for a needle in a haystack, risk assessment, budget, technology selection, operation locations, strategies and techniques all represent haystacks covering the potential border crime that we are trying to prevent. The nature of the Jordanian border is sandy loam in texture and generally devoid of vegetation making it suitable for sign-cutting in aerial surveillance, especially for the immediate concerns of recent smuggling of drugs and weapons operations across the Syrian border into Jordan, which have been identified by the Ministry of Foreign Affairs as a threat to national security, emphasising that Jordan will continue to confront this danger and the criminal groups behind it.

Theses in this work conclude that UAVs can provide critical surveillance value that cannot be substituted by satellites, aerial balloons, or fixed and mobile ground sensors, leaving the arguments of performance efficiency comparable to only manned aerial surveillance, comparing the total cost per flown hour of the two systems, specific advantages such as endurance & manoeuvrability, and the objective of minimising human power and human risk.

The author accepts Hypothesis 1 proven, which posits that “Utilising UAVs equipped with advanced sensors and processors can enhance the surveillance of lengthy perimeters, supporting their ongoing use in border security from a cost-benefit perspective”. For most applications, the high and advanced sensors are not affordable in the case of a fixed on the ground scenario, mobile on the ground also limits the range and the speed of scanning.

By 2024, there were many reported cases of UAVs either crashing, being jammed or shot down, as well as incidents of hacked information. Despite the lack of significant data on border surveillance UAVs, we could judge by the industry metrics, comparable to similar autonomous vehicle and manned surveillance systems. Therefore, the author accepts Hypothesis 2 proven, which posits that “The cyber-physical security of a perimeter surveillance UAV system can be managed to achieve a predefined level of security, ensuring resilience against potential threats”. I have shown that UAV systems are not necessarily riskier to fly if similar budgets are invested in the capabilities available to manage their cyber-physical security.

The author accepts that Hypothesis 3 has been proven, which states that "Machine vision can be used to detect clues to assist in the automation of the sign-cutting process in perimeter surveillance image data". Despite the limited data tested, an automated intensity-based image registration algorithm can filter out a large amount of images and quantify how much a particular scene frame has changed from the last scan, allowing the user to set a threshold at which level of change must be further analysed, this could help analysts to allocate their attention accordingly and mark a milestone to build on and develop further. Identified in Chapter 4. are the main clues that needed to be detected by an automated algorithm.

As this is a new topic, the open literature has very limited data on the accuracy of sign-cutting clues recognition by machine vision algorithms, urging the need for a benchmark dataset to train and test recognition algorithms and produce a measurable level of accuracy of the process. Therefore, the author rejects Hypothesis 4, which posits that “Perimeter surveillance UAVs can operate autonomously, and detect the majority of sign-cutting clues of intrusion using electro-optical imaging systems”. A reliable detection model is one in which the system is able to recognise clues in a standardised way of measuring the performance, for instance, the Top-5 accuracy is a measure of how often a model's top five answers match the expected answer, which is common in the field of machine vision.

9. Author Publication

1. Publications Related To The New Scientific Results.

R1. Al-Bkree, M. (2023). Managing the cyber-physical security for unmanned aerial vehicles used in perimeter surveillance. International journal of innovative research and scientific studies, 6(1), 164-173, DOI: 10.53894/ijirss.v6i1.1173.

R2. Al-Bkree, M. (2021). Optimizing Perimeter Surveillance Drones to enhance the security system of unmanned aerial vehicles. Security science journal, 2(2), 105-115, DOI: 10.37458/ssj.2.2.7.

R3. Al-Bkree, M. (2020). Slat armor to protect critical infrastructure. Military Technique, 54(3), 17–19, DOI: 10.23713/HT.54.3.03.

R4. Al-Bkree, M. (2019, August). Man-Tracking and Sign Cutting by Surveillance UAV. In 2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI) (pp. 253-256). IEEE, DOI: 10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00086.

2. Other Publications

R5. Issa, H., Al-Bkree, M., & Tar, J. K. (2022). On Certain Noise Filtering Techniques in Fixed Point Iteration-based Adaptive Control. SYSTEM THEORY, CONTROL AND COMPUTING JOURNAL, 2(2), 9-16, DOI: 10.52846/stccj.2022.2.2.38.

References

1. Zureik, E., & Salter, M. (Eds.). (2013). Global surveillance and policing. Routledge.
2. Mazzeo, A. (2021). Border surveillance, drones and militarisation of the Mediterranean. State Watch.
3. Dijstelbloem, H. (2021). Borders as infrastructure: The technopolitics of border control. MIT Press.
4. Aizeki, M., Boyce, G., Miller, T., Nevins, J., & Ticktin, M. (2021). Smart Borders or a Humane World?. The Immigrant Defense Project's Surveillance, Tech & Immigration Policing Project and the Transnational Institute.
5. Martínez, D. E., Heyman, J., & Slack, J. (2020). Border enforcement developments since 1993 and how to change CBP. Center for Migration Studies of New York (CMS) and the Zolberg Institute on Migration and Mobility at the New School.
6. Jeandesboz, J. (2011). Beyond the Tartar steppe: EUROSUR and the ethics of European border control practices. A threat against Europe, 111-132.
7. Bellanova, R., & Duez, D. (2016). The making (sense) of EUROSUR: How to control the sea borders?. EU borders and shifting internal security: Technology, externalization and accountability, 23-44.
8. European Council. 2013.Regulation (EU) No. 1052/2013 of the European Parliament and of the Council of 22 October 2013 establishing the European Border Surveillance System (Eurosur). Official Journal of the European Union56 (L 295): 11–26
9. The 2012–2016 Border Patrol Strategic Plan is available from U.S. Customs and Border Protection (CBP) at http://www.krgv.com/files/2012-2016_BP_Strategy.pdf (accessed, July 10, 2023).
10. Koslowski, R. (2021). Drones and border control: An examination of state and non-state actor use of UAVs along borders. Research Handbook on International Migration and Digital Technology, 152-165.
11. Bunker, R. J., Sullivan, J. P., & Kuhn, D. A. (2021). Use of weaponized consumer drones in Mexican crime war. Small Wars Journal, 70-71.
12. Kar, D., & Spanjers, J. (2017). Transnational crime and the developing world. Global Financial Integrity, 53-59.
13. Blanding, M. (2015). Workplace stress responsible for up to $190 B in annual US healthcare costs. HBS Working Knowledge; Forbes: Jersey City, NJ, USA.

14. Squire, V. (2014). Desert ‘trash’: Posthumanism, border struggles, and humanitarian politics. Political Geography, 39, 11-21.
15. Vernon, V., & Zimmermann, K. F. (2021). Walls and fences: A journey through history and economics. In The economic geography of cross-border migration (pp. 33-54). Springer, Cham.
16. Boyce, G. A. (2016). The rugged border: Surveillance, policing and the dynamic materiality of the US/Mexico frontier. Environment and Planning D: Society and Space, 34(2), 245-262.
17. Scott, B. I., & Andritsos, K. I. (2023). A Drone Strategy 2.0 for a Smart and Sustainable Unmanned Aircraft Eco-System in Europe. Air and Space Law, 48(3).
18. Szabolcsi, R. (2020). 3D flight path planning for multirotor UAV. Review of the Air Force Academy, (1), 5-16.
19. Snow, C. Making Sense of Drones. “http://droneanalyst.com/2014/02/06/making-sense-of-drones”. Accessed March 20 2022.
20. Muin, M. A., Kapti, K., & Yusnanto, T. (2022). Campus Website Security Vulnerability Analysis Using Nessus. International Journal of Computer and Information System (IJCIS), 3(2), 79-82.
21. Handa M. (2017, Jan 02) House Fire 1-2-17 Recorded on the Nest Camera [Video]. YouTube. https://www.youtube.com/watch?v=yHfoMrge4Zg&t=236s
22. Forum user, mourad27. (n.d.). Armee jordanienne / Jordanian Armed Forces. Far-Maroc Forum. https://far-maroc.forumpro.fr/t455p250-armee-jordanienne-jordanian-armed-forces.