ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORAL (PH.D.) THESIS

MAHMOD AL-BKREE

UNMANNED AERIAL SYSTEMS APPLIED TO SOLVE SAFETY AND SECURITY PROBLEMS

Scientific Supervisor
Prof. Dr. habil. Róbert Szabolcsi

09 October 2024

DOCTORAL SCHOOL ON SAFETY AND SECURITY SCIENCES

Public Defense Committee:

President:

Prof. Dr. Tibor János Goda

Secretary:

Dr. Judit Lukács

Members:

Dr. Ildikó Molnár

Dr. Zoltán Dudás

Prof. Dr. Endre Ruszinkó

Reviewers:

Dr. Bertold Békési

Dr. Mátyás Palik

Date of the Public Defense:

2025

DECLARATION

I am Mahmod Al-Bkree, a student of Bánki Donát faculty of the Doctoral School on Safety and Security Sciences, Óbuda University. I hereby declare that this Ph.D. thesis entitled "Unmanned Aerial Systems Applied to Solve Safety and Security Problems" was written by myself, except where cited in the references or the appendixes. I also certify that this thesis is an original report of my work and it has not been submitted anywhere for other qualifications or professional certifications.

Signature: Mahmod Al-Bkree

Budapest February 2025

ACKNOWLEDGEMENTS

I would like to thank the people who supported me during this research, and my special thanks and appreciation to my supervisor Prof. Dr. habil. Róbert Szabolcsi for his valuable help in guiding me during this research, without his support and guidance this research would not be possible.

Also, I would like to thank the staff of Obuda University, especially the Doctoral School on Safety and Security Sciences and my colleagues who worked with me and co-authored some of the published papers on the topic, as well as my family for their continuous encouragement and support.

Special thanks to the Hungarian people and the Stipend Hungaricum Scholarship program, for their amazing hospitality and cooperation. I have many people to thank for being part of this research and I want to pay my respect and gratitude to everyone who made this process possible.

List of abbreviation

AES	- Advanced Encryption Standard
API	- American Petroleum Institute
ASTM	- American Society for Testing and Materials
AUSEA	- Airborne Ultra-light Spectrometer for Environmental Application
AIS	- Automatic Identification System
BLoS	- Beyond the Line of Sight
CBP	- Customs and Border Protection
CCD	- Charge Coupled Device
CNN	- Convolutional Neural Network
CMOS	- Complementary Metal Oxide Semiconductor
CNRS	- National Center for Scientific Research (France)
CVE	- Common Vulnerabilities and Exposures
DoS	- Denial of Service
EUROSUR	- European Border Surveillance System
EO/IR	- Electro-Optical/Infrared
FLIR	- Forward-Looking Infrared
GCS	- Ground Control Station
GC/MS	- Gas Chromatography–Mass Spectrometry
GNSS	- Global Navigation Satellite System
GPS	- Global Positioning System
GSD	- Ground Sensing Distance
HALE	- High Altitude Long Endurance
HFWA	- Hybrid Fuzzy-Weighted Average
IMU	- Inertial Measurement Unit
IWW	- First World War
LC	- L1-signal Carrier
Li-Ion	- Lithium Ion
Li-Po	- Lithium Polymer
LOS	- Line-of-Sight
LPS	- Local Positioning System
LWIR	- Long-Wave Infrared
MILP	- Mixed Integer Linear Programming
MITM	- Man-in-the-Middle
ML	- Machine Learning
MOAS	- Migrant Offshore Aid Station

MOX	- Metal Oxide Semiconductor
MSF	- Médecins Sans Frontières
MR-SVM	- MapReduce and Support Vector Machine
NiCad	- Nickel Cadmium
NiMH	- Nickel Metal Hydride
OIC	- Object Installer Capability
PBSC	- Physical/Biological Samples Collectors
PPI	- Pixels Per Inch
PVA	- Position, Velocity, and Attitude
SAR	- Synthetic Aperture Radar / Search And Rescue
SNR	- Signal-to-Noise Ratio
SSIM	- Structural Similarity Index Measure
TC	- Timing Channel
TCHM	- Tele-Communication Human to Machine
TNT	- Trinitrotoluene
UAV	- Unmanned Aerial Vehicle
UAVSAR	- Uninhabited Aerial Vehicle Synthetic Aperture Radar
UWB	- Ultra-Wideband
USBP	- US Border Patrol
USD	- United States Dollar
VTOL	- Vertical Take-Off and Landing
WPA	- Wi-Fi Protected Access®
YOLO	- You Only Look Once
LSVRC	- Large Scale Visual Recognition Challenge

List of Figures

Figure 1. Illustration of border protection technologies……………………………………….. 19

Figure 2. The map shows the geo-political location of north-west Jordan …………….……..…… 26

Figure 3. Early UAV design, called Aerial Target 1916 ………………………………….……..... 27

Figure 4. Fixed-wing aircraft vs. helicopter vs. a possible hybrid-VTOL aircraft …………….. 28

Figure 5. UAV Diversity ……………………………………………………………………….. 29

Figure 6. UAV Energy Sources volume and mass-specific ………….…………………...…. 30

Figure 7. Global UAV market share 2020 by area of application in US$ billion …………...… 32

Figure 8. Response time to avoid collision ……………………………………...…………... 35

Figure 9. Frontex map of illegal border crossing ……………………………………………..… 37

Figure 10. UAV deployed by the EU Border Agency over the Mediterranean ……………..…. 38

Figure 11. Block diagram of a UAV system ……………………………………………...….… 44

Figure 12. Omni-directional vs directional antennas propagation ……………………...….... 48

Figure 13. Propagation patterns of directional antennas are electronically steered, and

simulated at different phases ……………………………………………...….. 49

Figure 14. An overview of the Nessus vulnerability scan report ……..……………..…....… 50

Figure 15. Shows the machine model identifying the highest difference between {A}&{B}

highlighting a sign of a potential suspicious event ……………………..………. 53

Figure 16. Signals spoofing attack illustration …………………………………..…………..… 55

Figure 17. The integration mechanism of two positioning methods to determine position, velocity, and attitude PVA ……………………………………………...…….…… 56

Figure 18. Illustration of Ultra-Wideband (UWB) ranging positioning system ……….……... 58

Figure 19. An aerial photo showing some of the damages on the oil processing facility …..... 62

Figure 20. An illustration of a crash test for fence rating ……………..…………...…… 63

Figure 21. Shows some transformed images from the original scene ……………………...…. 68

Figure 22. Velocity vectors and static pressure values on a multirotor UAV body ………..….. 69

Figure 23. Distorted airflow caused by the multirotor UAV and its effect on the gas plumes…70

Figure 24. Tire impression near the U.S-Mexico border ……………………………….…... 72

Figure 25. The thermal shadows ……………………………………………………….… 74

Figure 26. Flowchart illustration of a scanning mission ………………………………………. 76

Figure 27. Illustration of vertical air sampling ………………………………………………… 78

Figure 28. Detecting an object that was added to the scene during the unsurveilled period ….. 80

Figure 29. Shows the detected sign by image registration model ……………………..…… 81

Figure 30. Refreshing the road soil so footprints show up more easily ……………………….. 83

Figure 31. US Army transition from manned to unmanned aerial vehicles ……………….…. 86

Figure 32. Topography of Jordan ……………………………………………………………… 88

Figure 33. Electro-optical/infrared camera used for aerial imaging …………………………… 90

Figure 34. Principle of (a) colour and (b) monochrome CMOS camera …………………...….. 91

Figure 35. Wide portions of UV and IR wavelengths detectable by sensors ……….………..… 92

Figure 36. The appearance of grid lines from different lens orientations …………….……… 93

Figure 37. Difference between flat terrain imaging, and variable terrain imaging …….…..…. 94

Figure 38. Detecting chemical signatures in Hyperspectral image array ……………..….… 95

Figure 39. Visual image (left) spectral image (right) of a newly disturbed soil …………..….. 96

Figure 40. SAR image showing four detected humans ……………………………...…. 97

Figure 41. The development of commercial UAV 2017-2022 …………..……..…………...100

Figure 42. Illustration of the UAV operational ground area around the border line ……….... 103

Figure 43. Map of the Royal Jordanian Air Force bases distribution …………….…………106

List of Tables

Table 1. The estimated annual value of different transnational crimes ...……………….....……. 20

Table 2. Evaluation of surveillance and security technologies based on operators' subjective perception ……………………………….....……………………...…… 23

Table 3. Criteria to compare multiple UAV options ……………………………..…...…….. 34

Table 4. Shows the typical application of SAR at different wavelengths ……………..…....….. 98

Table 5. Sensors payload characteristics ……………………………………..……….……. 102

Table 6. Samples of technologies costs and operational values ………………...………..….. 108

Table 7. Sensor operational value evaluation used for ILP Model B …………..…………..…. 109

TABLE OF CONTENT

List of abbreviation **5**

List of Figures **7**

List of Tables **10**

TABLE OF CONTENT **11**

1. INTRODUCTION **13**

1.1. Background 14

1.2. Rationale for UAV Systems 14

1.3. Research Objectives and Scope 14

1.4. Hypotheses 15

1.5. Overview 15

2. LITERATURE REVIEW **17**

2.1. Transnational Crime 19

2.2. Qualitative Scale 22

2.3. Borders 23

2.4. UAV Systems 26

2.5. The Current State of Border UAVs 35

2.6. Observation and Contribution 38

2.7 Conclusion 40

3. MANAGING THE CYBER-PHYSICAL SECURITY FOR UNMANNED AERIAL VEHICLES USED IN PERIMETER SURVEILLANCE **42**

3.1. Background of Cyber-Physical Vulnerabilities 42

3.2. Suggested Solutions 46

3.2.1. Supply Chain 47

3.2.2. Antennas Radiation 47

3.2.3. Network Mapping 49

3.2.4. Navigation System 50

3.2.5. Encryption 51

3.2.6. Machine Learning 51

3.3. GPS\GNSS Spoofing 53

3.4. Complementary Positioning Methods 55

3.4.1. Positioning Based on Inertial Measurement Unit (IMU) 56

3.4.2. Local Positioning System (LPS) 57

3.4.3. Positioning Based on Vision 58

3.4.4. Positioning based on other sensors 59

3.5. Physical threat protection 59
3.6. Conclusion 64
4. SIGN CUTTING AND IMAGE REGISTRATION 66
4.1. The Challenge 67
4.2. The Limitation 69
4.3. The Proposed Approach 72
4.4. Signs to look for 74
4.5. Discussion 81
4.6. Conclusion 84
5. CASE STUDY OF A PROPOSED SOLUTION: EXAMPLE OF JORDAN 86
5.1. Technologies Selection 88
5.2. The Design Aspects 102
5.2.1. ILP Model A 106
5.2.2. ILP Model B 107
5.3. Results and Conclusion 108
CONCLUSION 111
NEW SCIENTIFIC RESULTS 114
OUTLOOK AND FUTURE WORK 115
AUTHOR PUBLICATION 116
1. Publications Related To The New Scientific Results. 116
2. Other Publications 116
REFERENCES 117
Appendix (Larger size Figures 4, 6, 9, 14, 34, 37, 41) 134

1. INTRODUCTION

Nations spend massively on security, throughout history many of the biggest projects were for security purposes. The Great Wall of China, the Manhattan Project, the Atlantic Wall, the F-35 Strike Fighter, and even the Apollo Project are all expensive projects done by nations to reduce the risk of ultimately losing a war. When nations feel threatened, they will gather all resources and even borrow as much as they can just to survive. The Greek philosopher Plato argued that war is an inevitable feature of human coexistence and that it is more common than peace, this argument continues to be demonstrated in our history as Chris Hedges points out: “If war is defined as an active conflict that has claimed more than 1,000 lives, then of the past 3,400 years, humans have been entirely at peace for 268 of them, or just 8% of recorded history”.

Fortunately, humanity has come a long way into the era of peace and prosperity, as we see people of all kinds of backgrounds coming to a common understanding, international, interfaith, and interracial, families are becoming the norm, and communication between all people being the easiest in all of history, I am confident that the paradigm has shifted to the era of a common voluntarily evolving civilization.

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.

1.1. Background

The rise of security concerns to protect the outdoor perimeters of large facilities requires a complex and dynamic solution for the challenge, in terms of detection and identification and response time. Facilities encompassing critical infrastructure, residential communities, and international borders require a security paradigm that transcends the limitations of traditional manpower-dependent systems. Advances in data collection, storage, and processing are attracting researchers to try to implement them to cover the scope of perimeter surveillance and to counteract potential threats. Deterrence and prevention are the first steps in addressing security concerns, conventional security systems combined with cutting-edge technology, could overcome the inherent limitations both in the area size and quality of security, reliability, and cost-effectiveness. A transformative approach is required that is flexible and scalable to address the evolving security landscape where affordable surveillance can be expanded, but the time consuming image analysis is automated.

1.2. Rationale for UAV Systems

Amidst the challenges posed by large perimeter security, UAVs present themselves as a promising solution that could provide continuous covering. These autonomous flying platforms have evolved beyond their military origins and now offer versatile applications in civilian contexts. The compelling rationale for integrating UAV systems lies in their potential to improve security operations in terms of endurance and cost per kilometre, providing an adaptable solution. By mitigating the inefficiencies of traditional systems of fixed sensors and manned flights, UAVs offer a way to improve efficiency, reliability, and a more cost-effective security framework.

1.3. Research Objectives and Scope

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.

1.4. Hypotheses

Hypothesis 1: The use of UAVs equipped with advanced sensors and processors can enhance the surveillance of long perimeters, supporting their continued use in border security from a cost-benefit perspective.

Hypothesis 2: 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.

Hypothesis 3: Machine vision can be used for clue detection, to assist in automating the process of sign-cutting in perimeter surveillance imagery data.

Hypothesis 4: Perimeter surveillance UAVs can operate autonomously, and detect the majority of sign-cutting intrusion clues using electro-optical imaging systems.

1.5. Overview

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. This thesis is organised into four main chapters, each contributing to a holistic understanding of the application of UAVs in large perimeter security. Chapter 2 provides a literature review that provides insight into the existing body of knowledge and identifies research gaps. Chapter 3 explores the conceptual design of the cyber-physical security of the system, Chapter 4 discusses the utility of the sign-cutting and image registration technology, and Chapter 5 is a case study of the proposed design for the Jordanian border.

2. LITERATURE REVIEW

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].

In an attempt to involve the public communities to participate in the effort some projects have begun to link security sensors to public access, " BlueServo^{SM} deployed the virtual community watch, an innovative real-time surveillance program designed to empower the public to proactively participate in fighting border crime [9].

The BlueServo^{SM} virtual community watch is a free service consisting of a network of cameras and sensors along the Texas-Mexico border. This network feeds free live streaming video to the user's computer, which they can access by creating a free account at www.blueservo.net. Users will log on to the BlueServo^{SM} website and directly monitor suspicious criminal activity along the border via this virtual fence-sm [10].

Citizens can sign up as Virtual Texas Deputies^{SM} to participate in border surveillance through this social network. Virtual Texas Deputies^{SM} from around the country will monitor the streaming video from these cameras 24/7 and report any suspicious activity directly to the border sheriffs via email. All emails regarding suspicious activity are submitted anonymously" [11].

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 [12].

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 [12]. 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 [13]. 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 [14].

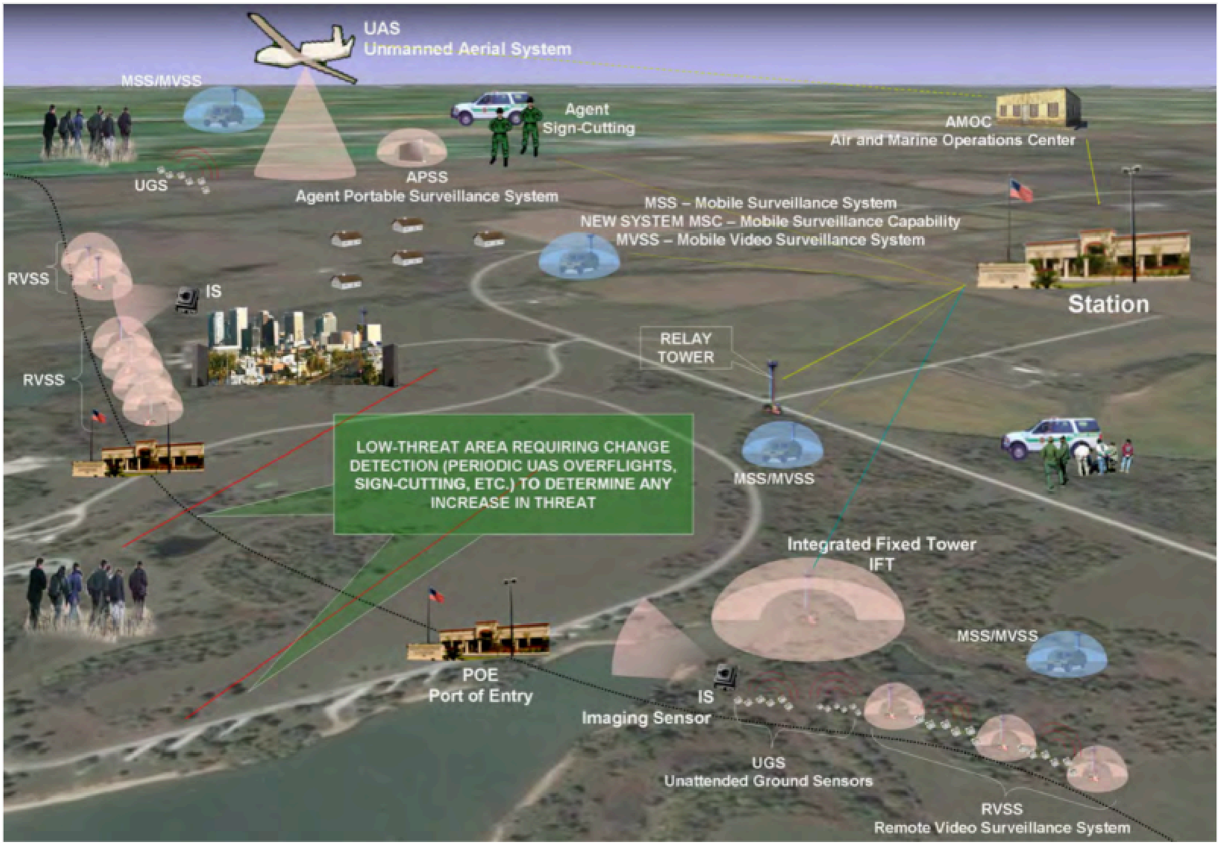
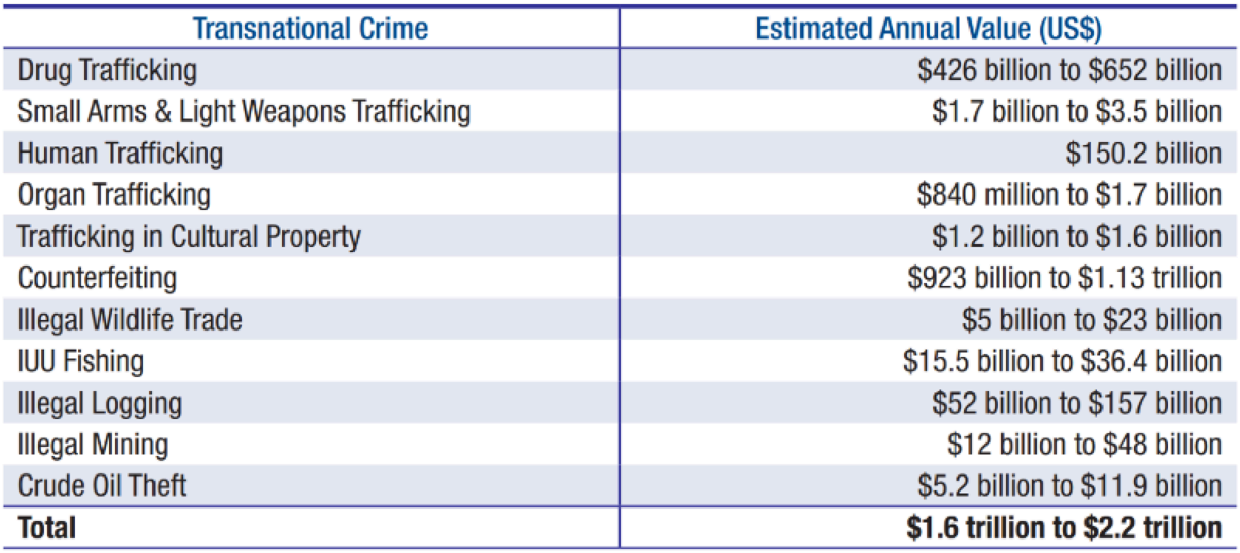

UAS
Unmanned Aerial System
MSS/MVSS
Agent
Sign-Cutting
AMOC
Air and Marine Operations Center
UGS
APSS
Agent Portable Surveillance System
MSS – Mobile Surveillance System
NEW SYSTEM MSC – Mobile Surveillance Capability
MVSS – Mobile Video Surveillance System
RVSS
IS
Station
RELAY
TOWER
RVSS
LOW-THREAT AREA REQUIRING CHANGE DETECTION (PERIODIC UAS OVERFLIGHTS, SIGN-CUTTING, ETC.) TO DETERMINE ANY INCREASE IN THREAT
MSS/MVSS
Integrated Fixed Tower
IFT
MSS/MVSS
POE
Port of Entry
IS
Imaging Sensor
UGS
Unattended Ground Sensors
RVSS
Remote Video Surveillance System

Figure 1. Illustration of border protection technologies [12]

2.1. Transnational Crime

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 [15] 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 [15]

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 [16], 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. [17] 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.

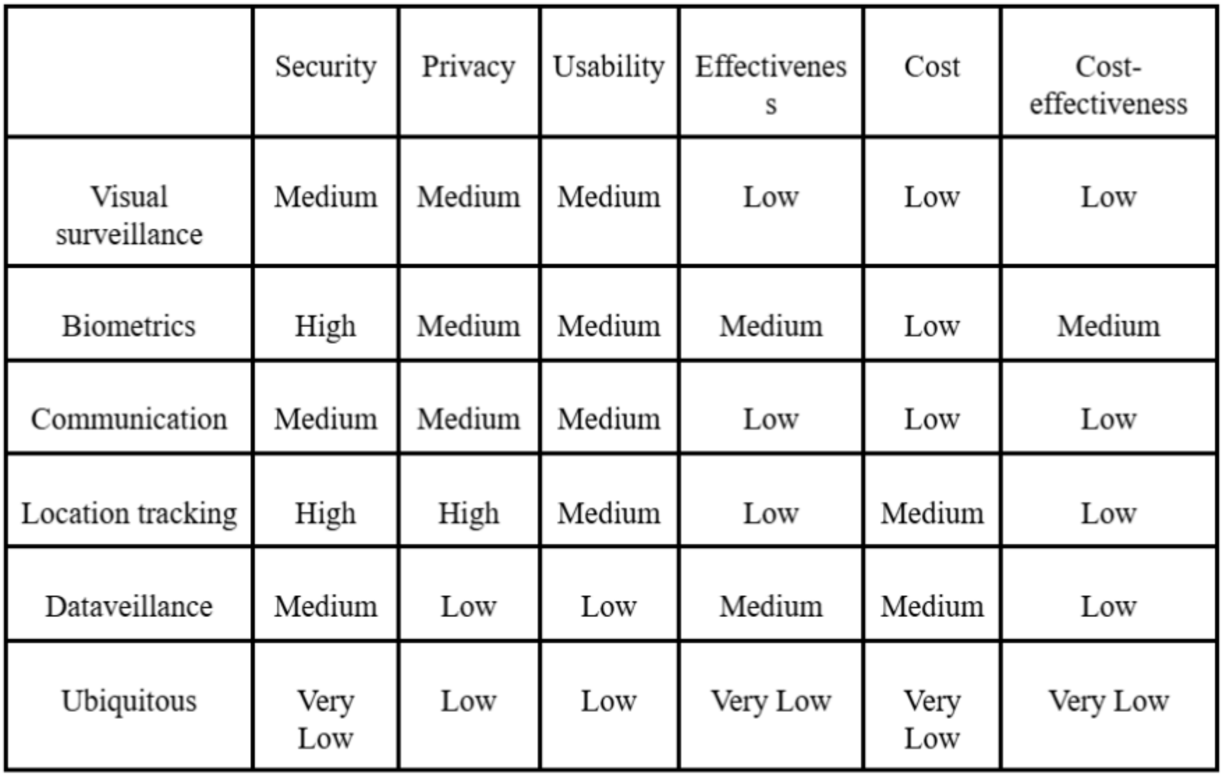
Basic measures such as fencing and low-tech surveillance can be at the lower end of the spectrum [18], while advanced technologies such as high-tech sensors, UAVs, and integrated monitoring systems can increase costs significantly. In addition, factors such as accessibility, environmental conditions, 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. [19] 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”.

It's important to note that the cost of border surveillance is a complex and multifaceted consideration, and the exact figures may vary depending on the unique circumstances of each border and the goals of the surveillance strategy implemented by the relevant decisions. Even the modernisation of legacy fencing in the United States is costly, averaging $5.494 million per mile [20], with surveillance cameras, access control systems, and personnel contributing to the overall expenditure [21]. The choice of technology and materials plays a key role in determining costs, with advanced systems often requiring substantial upfront investments but offering long-term benefits in terms of effectiveness and reduced maintenance [22]. In addition, the ongoing costs associated with monitoring and maintenance contribute to the overall cost of perimeter security,UAVs create a range of inseparable costs [23], and the news of a security system failure creates a wave of negative consequences around the globe [24]. Decision-makers must weigh the financial outlay against the potential risks and consequences of security breaches, as many breaches are an indirect result of failing to stop previous ones. Recognise that a well-implemented perimeter security system is an essential investment in protecting assets, personnel, and sensitive information [25]. As technology evolves, there is a growing emphasis on integrating cost-effective, scalable solutions that balance security needs with budget constraints [26], making it critical for decision-makers to carefully assess and prioritise their security requirements. Some technologies could have spin-off benefits such as using UAVs could reduce the inspection cost of energy infrastructures by half according to [27].

2.2. Qualitative Scale

While it is convenient to use estimated cost/benefits numbers, the complexity of calculating the cost of a security technology stems from a multitude of factors that extend beyond the initial purchase price [28]. First and foremost, there is the consideration of installation and integration expenses, which involve deploying the technology within existing infrastructures and ensuring seamless compatibility with other security measures. Ongoing operational costs, such as maintenance, updates, and personnel training, also contribute significantly to the total expenditure [29] & [30]. In addition, the dynamic nature of the security landscape necessitates anticipating future needs, potential upgrades, and evolving threats, introducing an element of unpredictability to long-term costs. Additionally, the intangible expenses related to the potential impact on business processes and productivity must be taken into account [31]. Balancing these factors requires a nuanced understanding of the specific security requirements, the scalability of the technology, and a comprehensive risk assessment. As security technologies become more sophisticated, the task of accurately estimating their total cost becomes more complex and requires a holistic approach that includes both immediate and long-term financial considerations. This can be a challenging process and can be estimated on an hourly basis (e.g., average cost of various methods) [32].

The subjective perception of security level involves a nuanced analysis of several key factors, including confidence, security, privacy, usability, effectiveness, and cost. Confidence in a security system is deeply intertwined with users' trust in its ability to prevent catastrophes. The sense of security hinges on the perceived strength of protective measures and the system's resilience against potential threats [33]. Privacy concerns come to the fore as users evaluate the extent to which their personal information is protected from unauthorised access [34]. Usability is critical, as an overly complex system may compromise overall security by relying on components that may become vulnerable. Effectiveness is gauged by how well the security measures respond to and mitigate real-world threats. At the same time, the risk of implementing and maintaining the security system is a key factor, as it influences the economic feasibility of its adoption [35]. Subjective perceptions of security thus result from a delicate balance among these interrelated components, highlighting the need for a comprehensive and user-centred approach to the design and implementation of security measures [36]. In a recent study, [37] evaluated surveillance and security technologies based on operators' subjective perceptions as shown in Table 2. below.



	Security	Privacy	Usability	Effectiveness	Cost	Cost-effectiveness
Visual surveillance	Medium	Medium	Medium	Low	Low	Low
Biometrics	High	Medium	Medium	Medium	Low	Medium
Communication	Medium	Medium	Medium	Low	Low	Low
Location tracking	High	High	Medium	Low	Medium	Low
Dataveillance	Medium	Low	Low	Medium	Medium	Low
Ubiquitous	Very Low	Low	Low	Very Low	Very Low	Very Low

Table 2. Evaluation of surveillance and security technologies based on operators' subjective perception [37]

2.3. Borders

Since the dawn of humanity, many civilizations have developed naturally in resourceful regions that were isolated from the "others", these regions allowed an easy movement and interaction internally and difficulties in being invaded by foreign armies, Egypt as an example provided fertile land along the Nile that did not need outside help to satisfy its basic needs, in terms of water and energy as well as the production of food, clothing, tools, and building materials.

Achieving a high level of sufficiency coupled with hundreds of kilometres of scorching desert isolating them from the outside enemies. Egyptians built an outstanding civilization that lasted around 30 centuries before the outsiders managed the logistics for a stronger army to pass Egypt's natural borders. [38] have mentioned that the ancient city of Jericho had a wall around the city. In the modern era, as [39] puts it, there are border disputes nearly all over the world making it inevitable that some security measures be used by all sides of a given border. Subsidising a foreign nation's borders could be considered an indirect border security policy, [40] specified "that Jordan will receive "not less than" $150 million from the Department of Defense's Operation and Maintenance, Defence-wide account for the Defense Security Cooperation Agency to reimburse Jordan for border security". The same act states up to $500 million for the Jordanian armed forces to use for border security.

Perimeter security is a historic continuous challenge, having a valuable resource increases the burden of protecting it [41]. As the facilities rapidly increase in both number and complexity, the advancement of modern technologies must be exploited to obtain an adequate level of protection, securing the overall facility especially when the risk endangers the extended operationality of the facility [42]. Today, there are many sites with large areas that fall into this range of long perimeters that need a high level of security (e.g. international borders, critical infrastructure, energy pipelines, rivers, and trade routes, etc.). Modern solutions for securing international borders, critical infrastructure, energy pipelines, rivers, and trade routes have evolved to integrate cutting-edge technologies and strategic approaches [43]. According to the European Commission [44], 50% of pipeline accidents are caused by external interference. Advanced surveillance systems, including high-resolution cameras, thermal imaging, and unmanned aerial vehicles, are improving real-time monitoring and situational awareness along international borders. Critical infrastructure, such as power plants and transport hubs, benefit from integrated security platforms that incorporate access control, biometrics, and artificial intelligence for threat detection [45]. Energy pipelines are protected by a combination of sensor networks, drone patrols, and satellite monitoring to detect potential breaches or anomalies [46]. Talarico in [47] evaluates the intrusion detection sensors by considering at least three key performance characteristics,

- the probability of detection (pod);
- the nuisance alarm rate (nar), consists in the alarms caused by factors other than an intrusion;
- the vulnerability is to be defeated or bypassed.

Rivers and trade routes are increasingly protected by intelligent navigation and communication systems, with technologies such as the Automatic Identification System (AIS) providing vessel tracking and maritime security [48]. Cybersecurity measures play a crucial role in securing critical infrastructure and trade routes, and safeguarding digital networks from potential threats, and some recent events have shown the vulnerability of these infrastructures [49]. In addition, international collaboration and information-sharing have become essential components of modern security strategies to effectively address transnational challenges [50]. The synergy of these modern solutions reflects a proactive approach to ensuring the security of global assets and maintaining the integrity of interconnected systems.

In 2001, the US and Canada declared the “Smart Border” where both nations agreed to enhance their cooperation on security practices [51], these practices have also been implemented by the US on the Mexican side of the border, as well resulting in improvements [52]. The Kingdom of Jordan's proactive approach to border security, as exemplified by the deployment of a smart border fence and advanced surveillance technologies, underscores the nation's commitment to protecting its borders and maintaining regional stability. The use of state-of-the-art surveillance systems, tailored to the country's unique geography and topography, reflects Jordan's understanding of the dynamic security landscape in the Middle East. As the country continues to invest in technological advances, it is poised to overcome challenges and serve as a model for effective border security strategies in the region [53]. Nonetheless, transparency and accurate reporting are seldom to be found in the case of Jordan as the military tradition is to prioritise security over accountability to the public opinion, and parliamentary committees audit military practices only under strict rules and limited official publication. The map in Figure 2. shows the geopolitical location of northwest Jordan as an example of a populated region with dynamic security considerations.

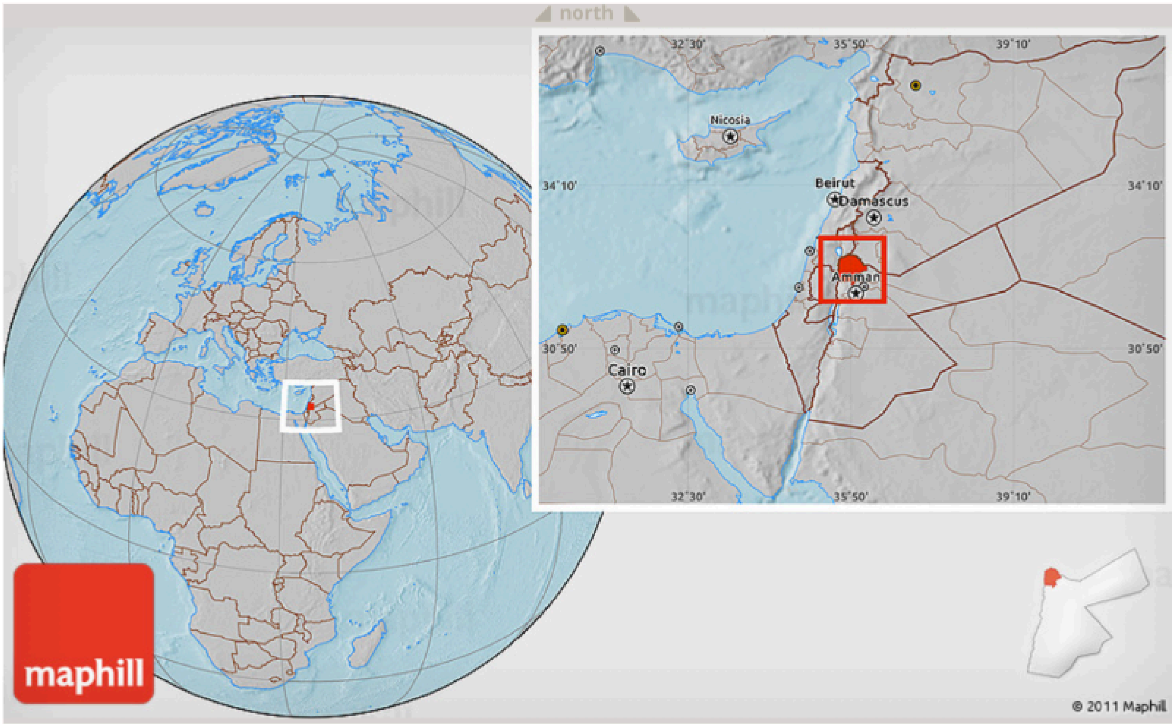


Figure 2. The map shows the geopolitical location of northwest Jordan [54]

While Jordan has not implemented complete persistent surveillance on its border, many advanced technologies are already in use along sections of the border in the four directions, the "military and the security apparatus fortified its borders after vast numbers of potential threat actors had left Jordan" [55].

2.4. UAV Systems

Unmanned Aerial Vehicles (UAVs), commonly known as drones, have emerged as indispensable tools for border surveillance, offering diverse capabilities to enhance monitoring and security [56]. The dynamic landscape of border challenges requires a variety of UAVs, each designed to meet specific requirements and operational environments [13]. Fixed-wing drones are characterised by their aerodynamic design, which resembles traditional aircraft. These UAVs are well-suited for covering large areas of borderland due to their extended flight endurance and higher speed capabilities which exceed 24 hours of flight time. Fixed-wing drones are often equipped with advanced imaging systems [57], enabling high-resolution aerial surveillance and efficient data collection and in many instances a communication link to ground bases or satellites. “The design of the first UAV is said to be associated with Prof. Archibald Low, the Air Minister of England. During WWI (the first World War) in 1916 he planned to apply against German-made Zeppelin-airships air torpedoes called Aerial Target (A.T.)” [58].

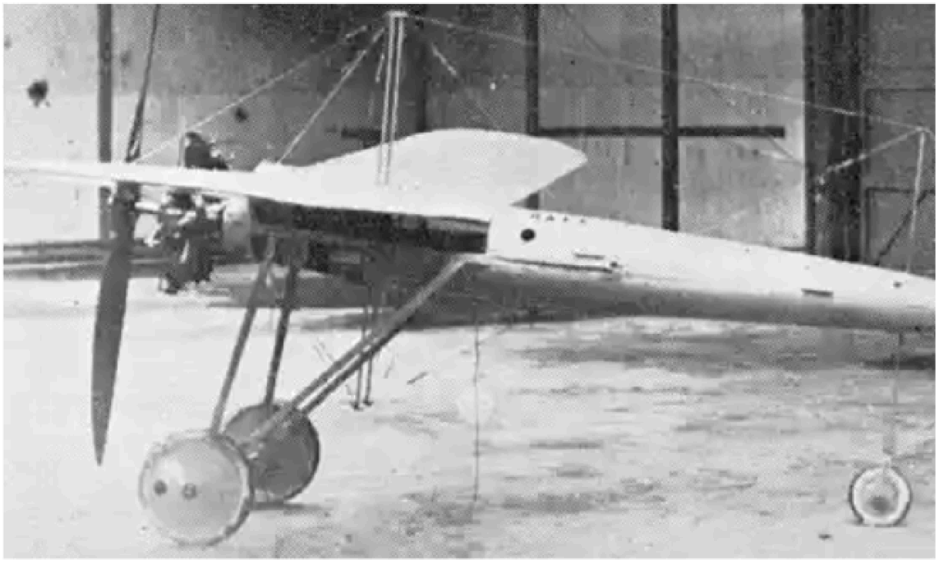
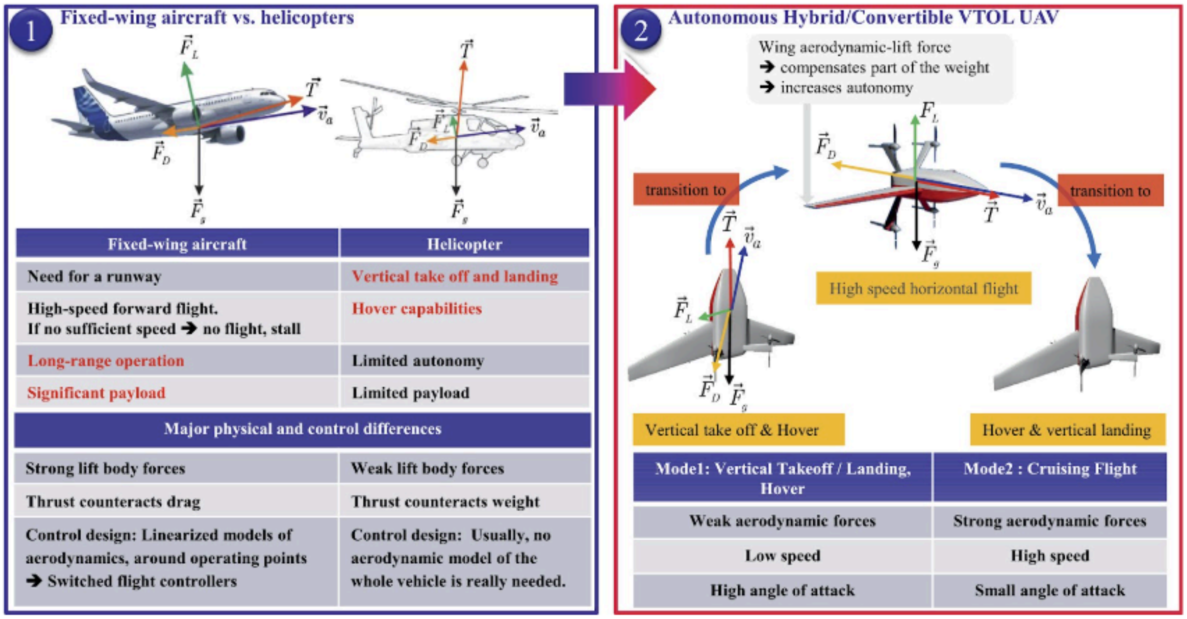


Figure 3. Early UAV design, called Aerial Target 1916 [58]

Rotary-wing UAVs, including the multirotor of quadcopters and hexacopters, are versatile and agile, making them ideal for close-range and intricate border surveillance missions. With the ability to hover and manoeuvre in tight spaces, rotary-wing drones are effective for monitoring border areas with challenging topography or dense vegetation. Often used for rapid response, situational awareness, and specific target observation, their manoeuvrability makes them a good choice to countermeasure other intruding UAVs. However, the endurance is usually much lower than that of fixed-wing UAVs, and also much less stable especially in windy situations, “Stability refers to the tendency of an object to remain in its present state of rest or motion despite small disturbances” [59].

For some applications that require vertical take-off and landing, VTOL drones combine the advantages of both fixed-wing and rotary-wing designs. They can take off and land vertically like a helicopter while transitioning to fixed-wing flight for efficient, long-range coverage.

VTOL drones are valuable in scenarios where flexibility and adaptability are paramount, allowing seamless deployment in a variety of perimeter environments. Hybrid-wing drones integrate multiple propulsion systems, combining the advantages of different UAV types. These drones are designed to optimise flight duration, speed, and payload capacity, providing a flexible solution for border surveillance missions. Hybrid drones are capable of vertical takeoff and landing, transitioning to fixed-wing flight, and then returning to vertical landing, enabling extended coverage with reduced operational constraints.

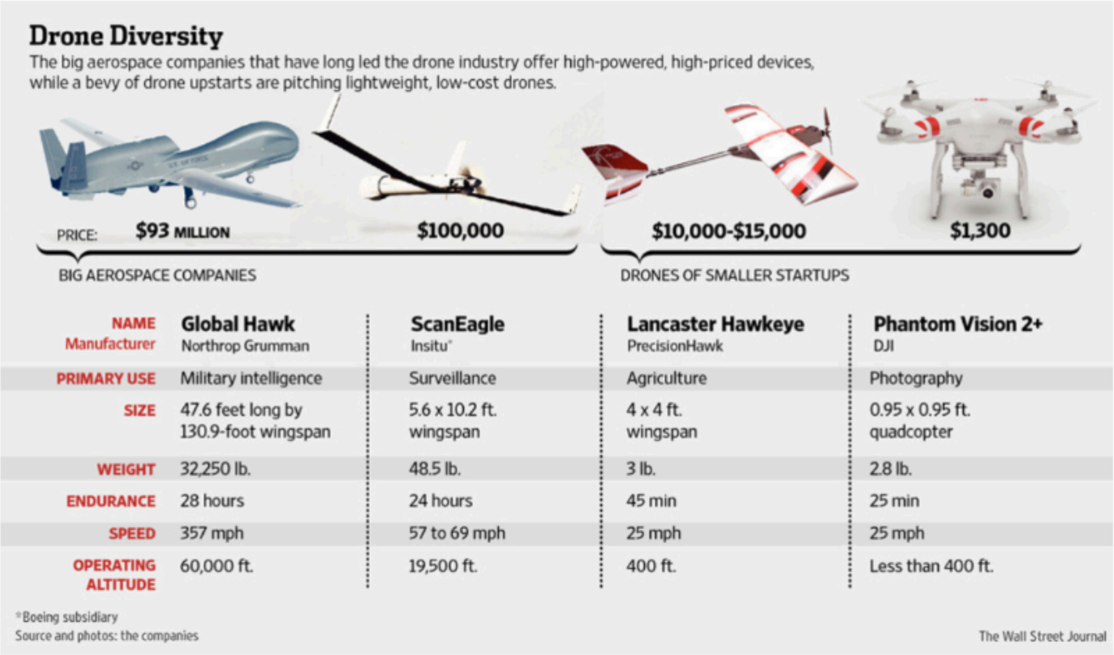


Fixed-wing aircraft	Helicopter
Need for a runway	Vertical take off and landing
High-speed forward flight. If no sufficient speed → no flight, stall	Hover capabilities
Long-range operation	Limited autonomy
Significant payload	Limited payload
Major physical and control differences	
Strong lift body forces	Weak lift body forces
Thrust counteracts drag	Thrust counteracts weight
Control design: Linearized models of aerodynamics, around operating points → Switched flight controllers	Control design: Usually, no aerodynamic model of the whole vehicle is really needed.

Mode1: Vertical Takeoff / Landing, Hover	Mode2 : Cruising Flight
Weak aerodynamic forces	Strong aerodynamic forces
Low speed	High speed
High angle of attack	Small angle of attack

Figure 4. Fixed-wing aircraft vs. helicopter vs. a possible hybrid-VTOL aircraft [60]

Another type is High Altitude Long Endurance (HALE) drones, which are designed to fly at high altitudes for extended periods, providing persistent surveillance capabilities. Equipped with advanced sensors and communications systems, these drones can monitor large border areas for extended periods, making them valuable for border patrols in hostile areas, intelligence gathering, and monitoring activities in remote or difficult regions. The variety of designs and variable costs allow decision-makers to choose from a full spectrum, many border patrolling agents carry a small UAV with a camera and a few other sensors at a cost of less than USD 1,000, and some of the continuously operated UAVs may require charging stations, “the Heisha charging station costs about USD 1,000, while a Mavic Air drone that can be charged by this station costs barely half the price at USD 600” [61].



Drone Diversity

The big aerospace companies that have long led the drone industry offer high-powered, high-priced devices, while a bevy of drone upstarts are pitching lightweight, low-cost drones.

PRICE: $93 MILLION
$100,000
$10,000-$15,000
$1,300
BIG AEROSPACE COMPANIES
DRONES OF SMALLER STARTUPS

NAME Manufacturer	Global Hawk Northrop Grumman	ScanEagle Insitu*	Lancaster Hawkeye PrecisionHawk	Phantom Vision 2+ DJI
PRIMARY USE	Military intelligence	Surveillance	Agriculture	Photography
SIZE	47.6 feet long by 130.9-foot wingspan	5.6 x 10.2 ft. wingspan	4 x 4 ft. wingspan	0.95 x 0.95 ft. quadcopter
WEIGHT	32,250 lb.	48.5 lb.	3 lb.	2.8 lb.
ENDURANCE	28 hours	24 hours	45 min	25 min
SPEED	357 mph	57 to 69 mph	25 mph	25 mph
OPERATING ALTITUDE	60,000 ft.	19,500 ft.	400 ft.	Less than 400 ft.

*Boeing subsidiary
Source and photos: the companies

The Wall Street Journal

Figure 5. UAV Diversity [62]

One of the most important criteria when selecting a UAV is altitude (metres). It's the capability of UAVs, it is a critical factor influencing their performance. Different UAVs are designed for various altitudes to meet specific mission requirements. Altitude affects Line-of-sight (LOS), communication range, and overall effectiveness in surveillance, reconnaissance, or other applications where the UAVs height above the ground is important.

Endurance (hours) refers to the length of time a UAV can remain in flight without refuelling or recharging. Longer endurance allows for extended missions and enhanced operational efficiency, making UAVs suitable for tasks requiring prolonged aerial surveillance, monitoring, or data collection. To enhance the endurance without compromising the payload the energy source of the UAV should be evaluated, adding more battery banks on board can extend the flight duration, [63] and [66] have compared Nickel Cadmium (Nicad), Nickel Metal Hydride (NiMH), Lithium Ion (Li-Ion), and Lithium Polymer (Li-Po) batteries and showed that Li-Po battery may be the most suitable selection primarily because it specific power of 2,800 watts per kilogram.

[65] recommend a hybrid power source stating that "UAVs have developed with a hybrid architecture of power supply incorporating batteries, fuel cells, solar photovoltaic systems, and supercapacitors for extended endurance and improved performance". Figure 6. below shows the UAV energy sources in terms of volumetric energy and mass-specific energy.

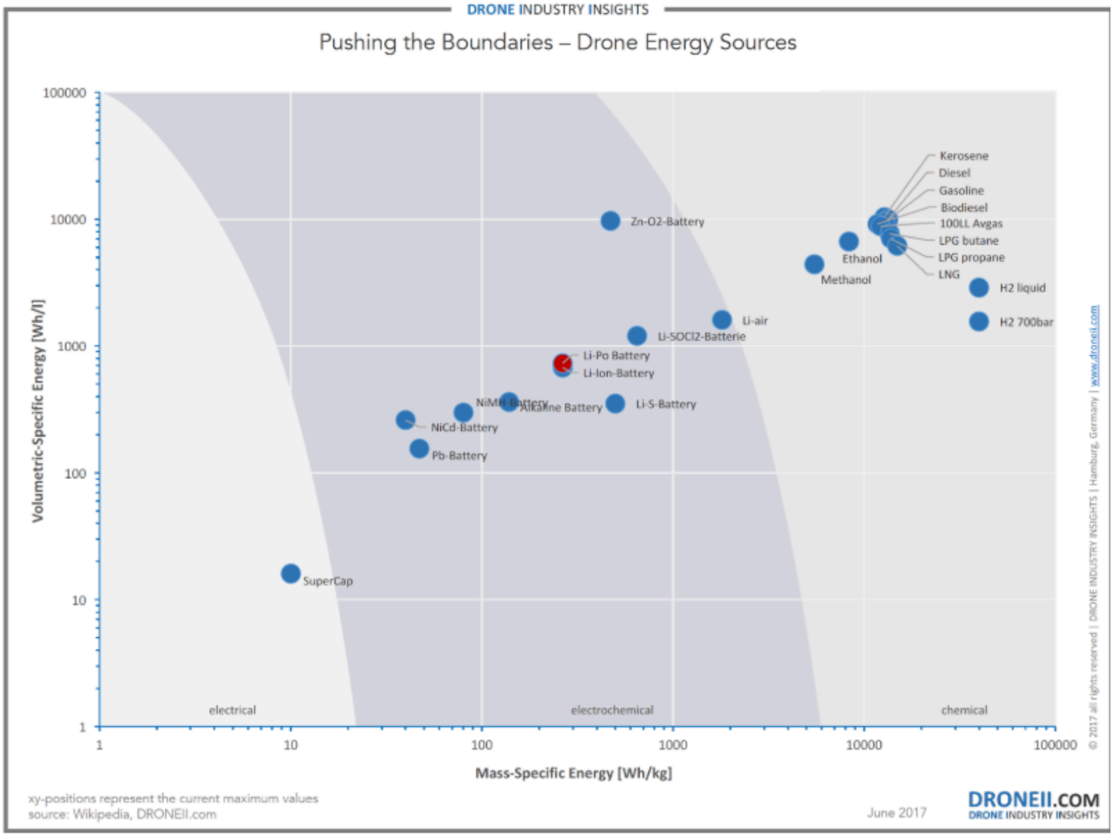


Figure 6. UAV Energy Sources volume and mass-specific [66]

Range is the maximum distance a UAV can fly from its launch point. A longer range increases the coverage area and flexibility of UAV operations, particularly in border surveillance, where extensive territories need continuous monitoring. "Endurance is the time that the aircraft can remain airborne before running out of energy" [59], and the more endurance a UAV has, the more area range it can cover at the same speed. The speed of UAVs affects their responsiveness and efficiency in covering large areas. Higher speeds are beneficial for rapid deployment, target tracking, and reduced mission completion time. Payload (kilograms), Payload capacity represents the weight a UAV can carry, including sensors, cameras, communications equipment, or other mission-specific tools. A higher payload capacity allows for the integration of advanced technologies and multiple sensors, usually, payload has an inverse relationship with the range. Speed can be critical in the event of an enemy attack or when tracking a target.

Some designs use morphing of the structure to improve flight endurance by gliding, generating the lift force that opposes their weight and keeps it in the air from environment air currents [64], other designs are dependent on a wireless electrical charging or onboard photovoltaic solar panels to supply the UAV with extra energy and improve its endurance. The cost of UAVs varies significantly (from a few hundred to millions of USD) based on factors such as technological sophistication, payload capacity, range, and endurance. The balance between cost and performance is crucial in optimising the efficiency of UAV deployments for specific applications usually by calculating the cost/value ratio.

According to [67], by 2026 the drone market is anticipated to register $40.7 billion. This is almost double the estimated market share in 2020. Figure 7. shows the estimated market share by area of application. American highly advanced unarmed UAVs are still only sold even to countries that are considered allies, encouraging countries such as Turkey to develop their own UAV technology and other countries to meet their needs from alternatives such as Chinese products. The nature of surveillance UAV applications makes them likely to perform better with international cooperation instead of protectionism and competition.

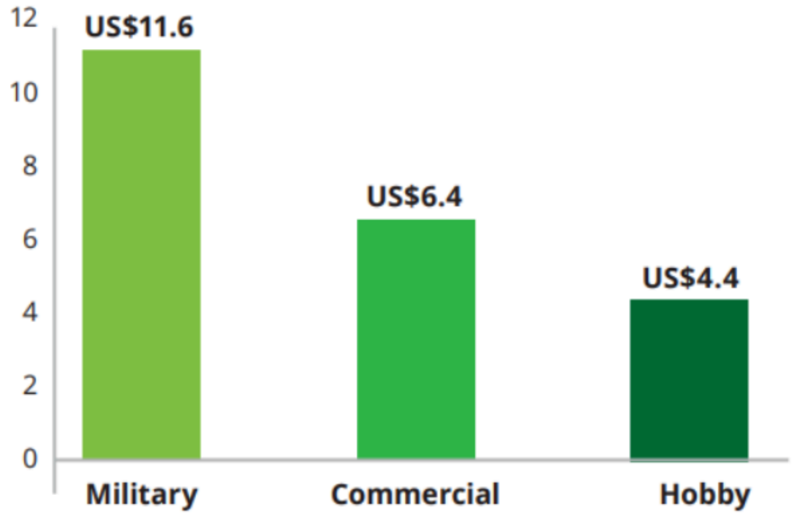


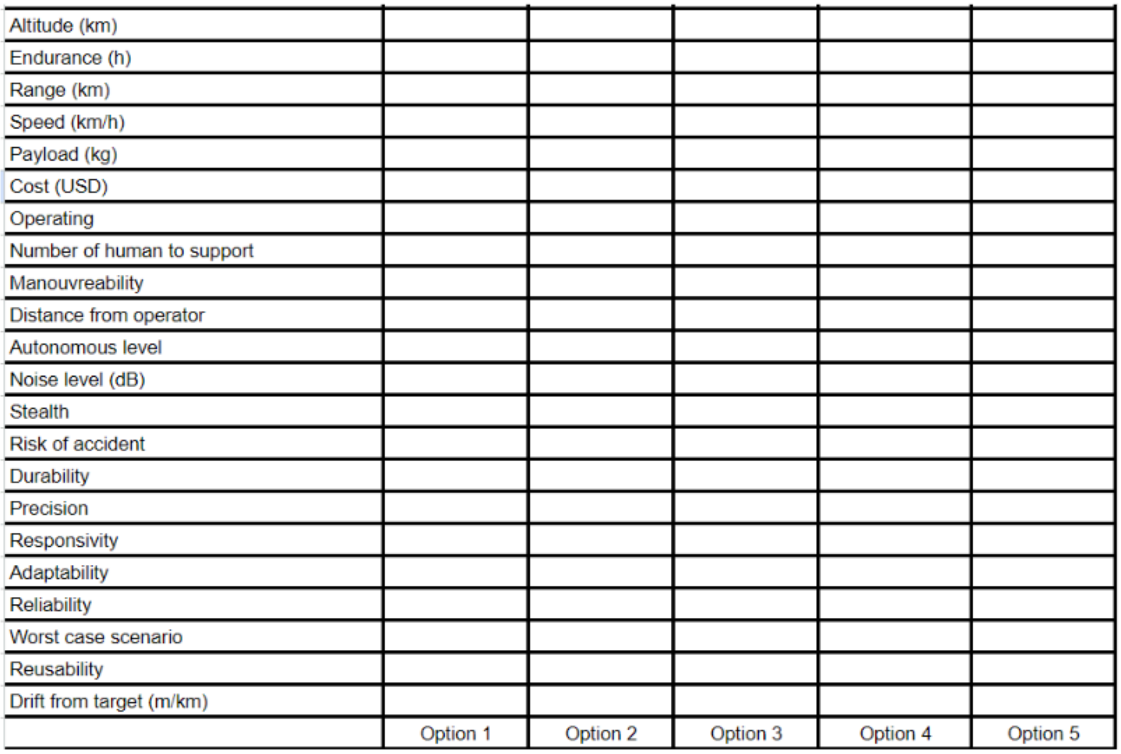
Figure 7. Global UAV market share 2020 by area of application in US$ billion [68]

The number of humans needed to support UAV operations including personnel involved in mission planning, launch, monitoring, maintenance, and data analysis would greatly vary depending on the mission and the level of autonomy of the system. Minimising the human support needed enhances the cost-effectiveness and efficiency of UAV operations and reduces human error. Manoeuvrability is critical for adapting to dynamic environments and responding to changing mission requirements. UAVs with high manoeuvrability can navigate complex terrains and execute precise movements, optimising their operational effectiveness. Also, it’s crucial for operations that countermeasure other intruding UAVs, manoeuvrability tends to affect and get affected by stability and it could be undesirable in some situations [59]. The distance from the operator represents how far a UAV can be operated remotely. Extended operating distances provide flexibility in deploying UAVs for missions across vast geographical areas. The autonomous level indicates the degree to which a UAV can operate independently without constant human intervention. Higher autonomous levels enable UAVs to execute complex tasks, navigate obstacles, and adapt to changing conditions autonomously. Noise level is a critical consideration, especially for covert or discreet operations. Lower noise levels reduce the risk of detection and interference, making UAVs suitable for surveillance or reconnaissance missions where stealth is essential, the opposite could be argued for some search and rescue missions.

Stealth features, such as low radar cross-section and minimal acoustic signature, enhance UAVs ability to operate covertly. This is critical for missions where avoiding detection is essential. Accident risk assessment involves evaluating factors such as collision avoidance systems, redundancy of critical components, and overall reliability. Minimising the risk of accidents is essential to ensure the safety of both the UAV and the surrounding environment.

Many of the small-medium sized UAVs used by civilians are used by some European groups, these groups include Migrant Offshore Aid Station (MOAS), Médecins Sans Frontières (MSF), Sea-Watch, and WatchTheMed. The activities of these groups have complicated the traditional understanding of European border zones as spaces where only the police and military conduct surveillance. These civilian groups also use surveillance technologies, including drones, aircraft, satellites, GPS, binoculars, radar, and other shipboard systems, to conduct or support search and rescue (SAR) operations and/or to monitor border authorities.

The durability of UAVs relates to their ability to withstand environmental conditions, harsh weather, and potential impacts. A durable UAV is more reliable for sustained operations in challenging terrain, with a reasonable need for regular maintenance. Precision refers to the accuracy and reliability of a UAV in executing tasks such as following a track, data collection, or payload deployment. The more precision allows for versatile missions requiring accurate and reliable results. Responsiveness measures how quickly a UAV can respond to commands or change the mission parameters in the middle of a mission. A highly responsive UAV is better able to adapt to dynamic situations and make rapid changes to its mission, helping it to avoid other objects. Adaptability is the UAVs capacity to integrate with different payloads, sensors, or technologies, allowing for customization based on the specific requirements of different missions, making it easier to upgrade, and more versatile for new designs.



Altitude (km)					
Endurance (h)					
Range (km)					
Speed (km/h)					
Payload (kg)					
Cost (USD)					
Operating					
Number of human to support					
Manouvreability					
Distance from operator					
Autonomous level					
Noise level (dB)					
Stealth					
Risk of accident					
Durability					
Precision					
Responsivity					
Adaptability					
Reliability					
Worst case scenario					
Reusability					
Drift from target (m/km)					
	Option 1	Option 2	Option 3	Option 4	Option 5

Table 3. Criteria to compare multiple UAV options [Author]

Reliability encompasses the overall dependability and consistent performance of a UAV. It's probably the most important criterion that ensures that the UAV can successfully complete missions with minimal downtime or malfunction.

Considering the worst-case scenario involves evaluating the UAVs ability to handle unforeseen challenges, system failures, or unexpected environmental conditions. As acknowledged in [70], part of the system design for the UAV H2 controller, this preparedness is critical to maintaining mission success under adverse circumstances. Reusability measures the extent to which a UAV can be recovered, maintained, and relaunched for subsequent missions. Reusable UAVs reduce overall operational costs and enhance sustainability, and crash avoidance increases the rating of reusability. Drift from the Target (metre/kilometre) indicates the deviation of the UAV from its intended path or target location over a certain distance. Minimising drift is vital for precision applications, such as surveillance or reconnaissance, where accurate positioning is essential. I strongly recommend multiple positioning methods which among their benefits reduce drift. These main parameters collectively shape the capabilities and effectiveness of UAVs in various applications [59], emphasising the need for a nuanced understanding of their specifications to align with specific mission requirements and operational contexts, weighing them is still to an extent a subjective task, to balance the overall performance. The reliability of some criteria works together to enhance certain functions and tasks. Speed, manoeuvrability, stability, and computing power would determine the response time for hazard avoidance, as illustrated in Figure 8.

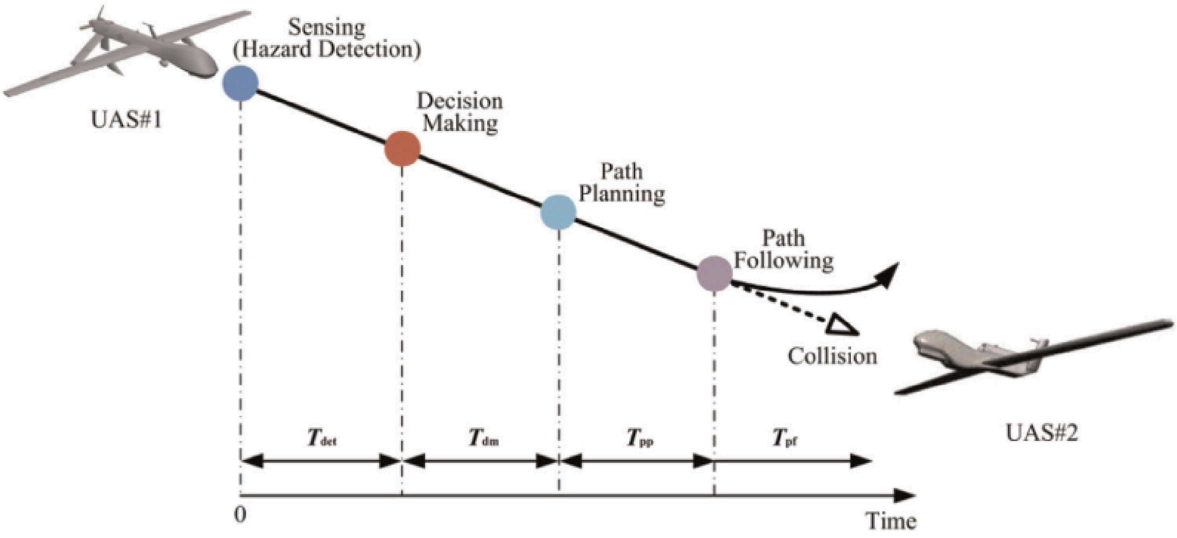


Figure 8. Response time to avoid collision [71]

2.5. The Current State of Border UAVs

Some advantages of using UAV for border security,

- UAVs would extend the benefits of the fixed cameras, and human patrols, dynamically covering more surveilled areas with different sun angles, leaving no blind spots;
- after detecting an intruder the UAV would have a fast and efficient first response, carrying a microphone and speaker to communicate with the intruder (also spotlight, siren, …etc);
- reducing human cost, error, and flexibility to change;
- initial cost of the system compared to the manned, and stealth of smaller UAVs.

The use of multiple UAVs for a unified mission is still facing many challenges starting from communication protocols between them [72]. In the last decades, there has been significant attention and discussion around the use of UAVs for military and civilian applications. The use of non-threatening UAVs for security purposes is receiving a great deal of attention. One noteworthy domain where this becomes evident is in the utilisation of drones for border control around the world by militaries, civil organisations, and private contractors. Loukinas in [73] studies the employment of UAVs by both state and non-state entities at the European border lines.

In many regions around the globe, drones are now deployed to patrol national borders. However, this practice may pose significant challenges to conventional notions of personal privacy and individual liberties [74]. Moreover, it gives rise to crucial legal, ethical, and moral inquiries regarding the integration of military technology into civilian society and data collection and processing. The deployment of drones in border control may even contribute to heightened military tensions in disputed border areas. For example, flying a drone close to a shared border with a neighbouring state in the midst of tense relations could be perceived as provocative, with potentially dangerous consequences, as in the case of the Indonesian-Malaysian border dispute in West Kalimantan [75]. The current landscape concerning the use of UAV systems for border surveillance and control can be noticed all around the world. Studying the practical and political challenges associated with employing such systems for these purposes, and addressing ethical concerns and potential risks. So we might find some benefits from the opportunities and challenges examined by several nations.

Since the turn of the century migration to the European Union has increased dramatically, the two major wars in Afghanistan and Iraq created a substantial wave of migrants, which encouraging people from many other Asian and African countries to take advantage of the situation and migrate to the European Union [76], this wave was followed by the wars in Syria, Yemen, and Libya creating massive challenges on the southern borders. The European Border Surveillance System (EUROSUR), established in 2013, is a framework for information sharing, and cooperation between Member States with agencies such as Frontex to create joint efforts and enhance the capabilities and increase control at the external borders. Many European agencies are collaborating by sharing data and tasks, using various tools and techniques including UAVs.

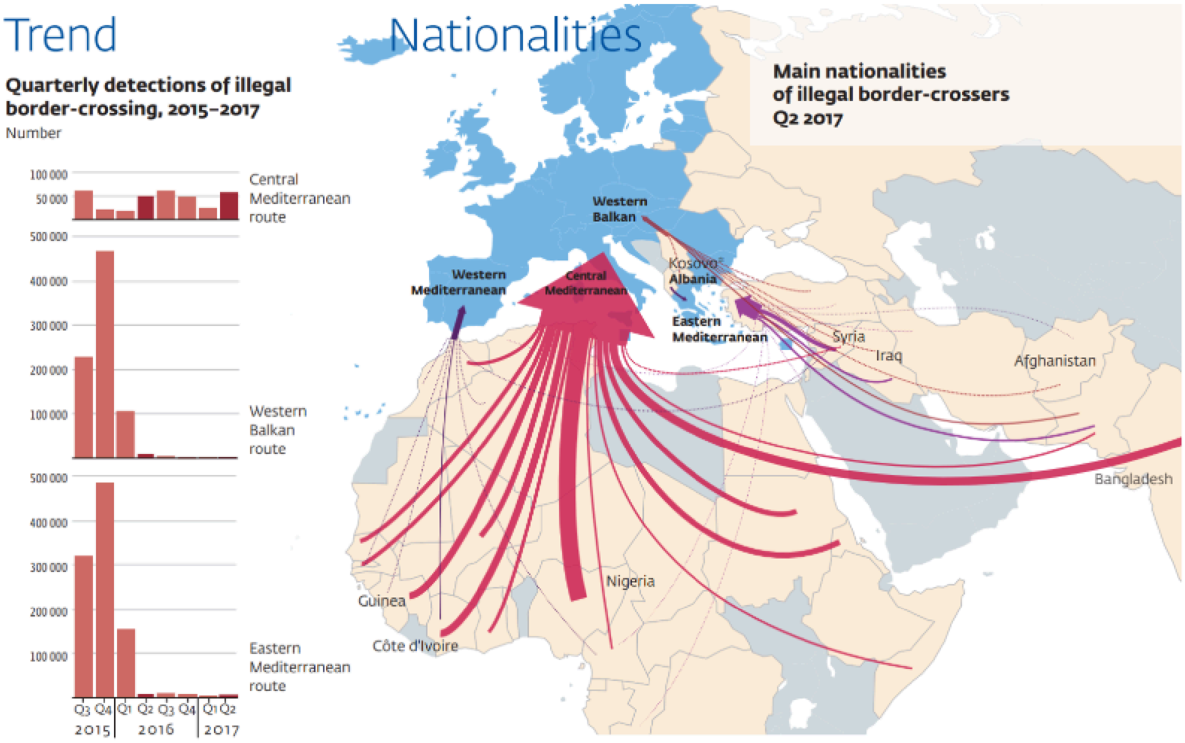


Figure 9. Frontex map of illegal border crossing [77]

Frontex, the European Border and Coast Guard Agency, has been setting up an aerial surveillance service since 2016 that includes UAV flights. They implemented fixed-wing, multi-rotor, and hybrid UAV systems to help EU member states fight cross-border crime [77]. In other situations where rules prevent the use of UAVs, an optionally piloted surveillance aircraft was considered by Frontex.

Figure 10. UAV deployed by the EU Border Agency over the Mediterranean [77]

The US military has been conducting operations on the southern border that include UAV systems such as the General Atomics MQ-1C Gray Eagle and others, However, but the Bureau of Customs and Border Protection (CBP) is the main entity that carries out the border security responsibilities and has utilised hundreds of UAV systems on its border patrols mainly the US Reaper, Predator, and Hawk UAVs, as well as a mall multirotor such as the UNID PU-9, Ravens UAV.

The Kingdom of Jordan has a continuing border challenge, with conflict tensions on the western border, illegal drug smuggling from the northern border, and the wars in Iraq and Syria causing criminal groups to cross the border into and out of Jordan. Another challenge is the limited defence budget. Jordan has used six of the Chinese-made CH-4 UAVs, but reports are limited and no publications have been found on the effectiveness and nature of their operations.

2.6. Observation and Contribution

In this chapter, we examine 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.

The first factor 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.

2.7 Conclusion

Although perimeter surveillance UAVs are a sensitive topic and many results are not disclosed or published for being classified information, there are hundreds of scientific papers published every year on the topic. It could be argued that the majority are exploratory in nature, or justify their use by the high potential for results in the near future. However, many researchers have clearly demonstrated the effectiveness of the approach especially in the field of detection and tracking in real-time, leaving scepticism only about the comparison between their performance and that of manned aircraft, arguing that the high rate of accidents and crashes which makes the overall cost over the lifetime of both systems similar in terms of cost per a flight hour. The high accuracy of detection, tracking, and action recognition proves the concept for live detection from one side, keeps the question of minimising flight hours by detecting passive signs open, and urges the need for new benchmark datasets to test and compare the performance of different machine vision algorithms and sign-cutting detection and tracking. By reviewing the available open literature, aerial surveillance is an effective and justified approach for perimeter security and the argument of the high crash costs compared to manned aerial vehicles has been diminished in recent years by the new models, therefore, the author finds that the majority of the surveyed related literature converges to support **Hypothesis 1.** On the other hand, the author believes that the system optimisation is likely to continue to accelerate at a rate faster than the acceleration rate of criminal capabilities.

3. MANAGING THE CYBER-PHYSICAL SECURITY FOR UNMANNED AERIAL VEHICLES USED IN PERIMETER SURVEILLANCE

This chapter highlights the vulnerabilities of perimeter surveillance unmanned aerial vehicles to cyber-physical security threats and discusses some approaches to manage them. As the majority of cyber threats to the UAVs come through their onboard wireless transceiver, we propose antennas propagation types that limit the vector of the threat, and also the importance of vulnerability scanners to assess the system risks. And to address the limited power and computing resources onboard, a computationally efficient onboard encryption method is proposed and a sign-cutting machine vision algorithm to provide warning of suspicious activity detected on an interrupted surveillance image.

3.1. Background of Cyber-Physical Vulnerabilities

Millions of new pieces of cyber malware are detected every week. Unmanned aerial vehicles (UAVs) have proliferated in many sectors ranging from less sensitive applications to higher-sensitive ones such as surveillance. The vulnerability of UAVs to cyber threats is similar to that of any computing device such as a smartphone or a modern internet-connected car. However, some specific characteristics of surveillance UAVs require management of their potential security vulnerabilities. In particular, critical infrastructure often deploys perimeter surveillance UAVs with the following characteristics:

- flown a repeatable predetermined path around the perimeter;
- the path is usually long (e.g. international border, energy pipeline…);
- surveillance is limited in time (e.g. one or few scans per day);
- exposed physical space and cyberspace.

Many of the advanced tools that are used to counter cybersecurity threats are the same tools used by malicious attackers, who are inventing new methods of reconnaissance, weaponization, delivery, exploitation, installation, command and control and targeting.

In the literature, researchers have done good work in identifying potential cyber attacks, and highlighting the need for new designs that minimise cyber threats. The work in this chapter aims to identify what are the main criteria of a UAV system that should affect the selection process from a cybersecurity point of view, and how we can utilise the specificity of UAV tasks to manage cyber threats (e.g. flying a predetermined path over known objects on the ground could allow navigation independent of the main GNSS attack space). Another notable research gap is that many papers have been published on identifying suspicious activity in an active scene, while very little research has been done on analysing passive scenes (e.g. sign-cutting using a passive scene).

Depending solely on third party providers could be itself a vulnerability, in house development of strategy and customization is recommended to keep the uncertainty dynamic of the system and reduce the attacker's knowledge of items, planning a unique operating system cryptography schemes, and cryptography, network security protocols, operating system mechanisms, database schemes to reduce the attacker's ability to exploit publicly available data and keep a moving target defence dynamic. An additional layer of protection that is impeded in the design assures having specialised advanced technology of a third-party solution together with a uniqueness of hybrid security layers, the cyber criminals are more likely to breach a generalised defence system, and many reports of hacking into commercial security cameras and commercial well known UAVs, as these systems are totally dependent on the manufacturer's security measures and its updates, investing in the development of additional layer of security would help the end user to better understand and exploit the full potential of the supplied defences to their optimal use [R1].

Factors such as scalability, integration, and periodic upgrades affect the overall cost of buying a mass-produced tool comparable to customising for specific cyber security requirements. The three-dimensional nature of UAV operations requires compromises to be made in certain methods to fit the onboard payload, computing power, memory, and energy consumption, forcing decision makers to find new ways to compensate the deficiency of onboard cyber defence hardware and software by redundancy in the Ground Control Station (GCS) and to achieve a cost effective solution that satisfies standard security requirements. Figure 11. shows a block diagram of a UAV system.

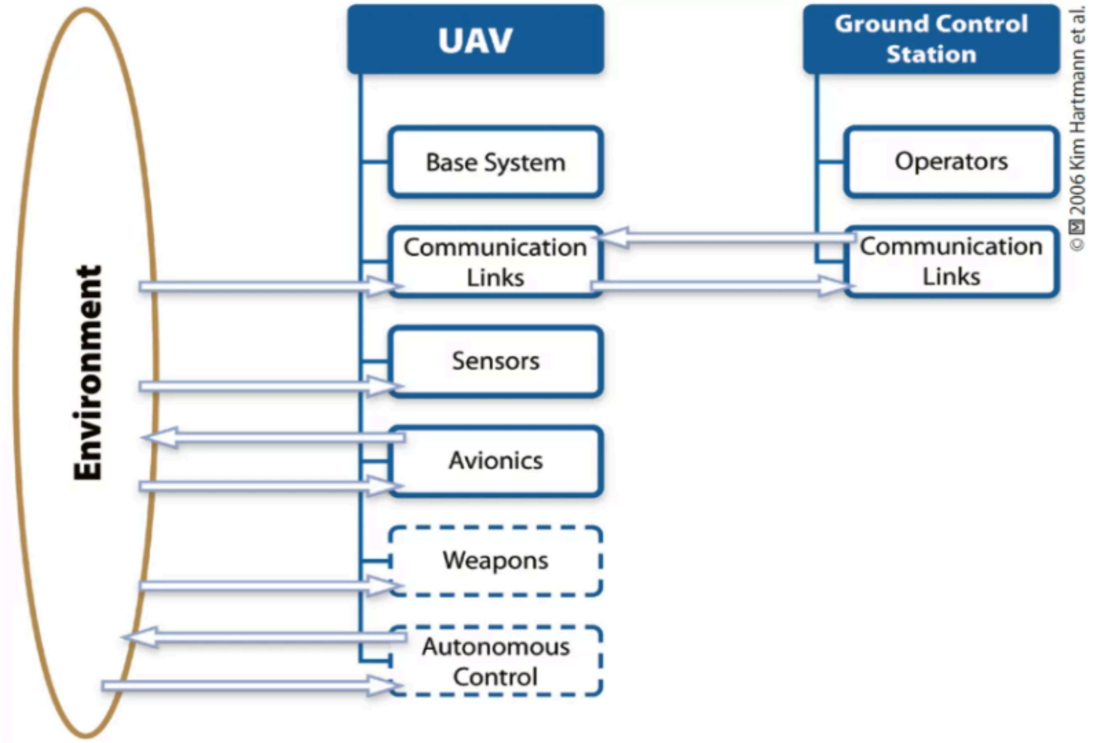


Figure 11. Block diagram of a UAV system [78]

Recently, there have been several different approaches to the meaning of UAV/UAS systems. In [79] a main and robust framework for the UAS was given, describing its main parts with further analysis. To get a UAV/UAS system with skills able to fly Beyond Line-of-sight (BLOS) strong flight automation is required, which is thoroughly evaluated by [79]. According to [80] "most cybersecurity vulnerabilities are based on sensors, communication links, and privacy via photos".

It is well-known that any certification of the UAVs often bumps into a lack of existing and widely accepted regulations. The scientific paper [58] first gave a set of performances proper to use to evaluate UAVs airworthiness. In more detail, Szabolcsi in [81] derived a set of dynamic performances of the UAV longitudinal motion, while in [82] he derived a class of dynamic performances proposed to be used to evaluate UAV lateral/directional motion dynamic performances.

UAVs are suitable for perimeter surveillance tasks because they can cover long distances and reach difficult areas at relatively high speeds [83]. A review of several known cybersecurity vulnerabilities and previous attacks was presented in the work of [84]. GNSS spoofing threats were evaluated in [85] and it was concluded that even though spoofing currently might be difficult to perform in the field at present, the low-cost GNSS jammers indicate that similarly low-cost GNSS spoofers will eventually be developed. The need for a balance between the security level of cryptographic protocols and their computational resource requirements can be seen in [86].

The management starts from the manufacturing stage and the supply chain, regulating the main components as stated in [87] "Internet of Things and cyber-physical systems comprise interacting logical, physical, transducer, and human components engineered for function through integrated logic and physics". Where it is important to design the infrastructure according to certain standards along the full supply chain "The virtual supply chain itself is a source of vulnerabilities and its resilience is only as good as the cybersecurity infrastructure that it employs" [88]. In their work. [89] have identified some key research gaps, and their paper "has presented a systematic survey of the extant literature on cybersecurity in logistics and supply chain management. The key findings are as follows:

1) Existing studies rarely use real-world cybersecurity data;

2) Studies focusing on cybersecurity in logistics are scarce although logistics plays an important role in supply chains;

3) There is only a limited number of papers adopting quantitative research approaches to study cybersecurity in logistics and supply chain management;

4) While a few studies focus on real-time recovery and aftermath measures, most studies focus on precautionary measures;

5) Blockchain technologies are still in their infancy in the transport and logistics sector;

6) Most studies use one-way encryption schemes that overlook the potential threats in a future dominated by quantum computing techniques;

7) Studies on information security and digital forensic investigation are scarce"

Cybersecurity must be treated as important as the traditional quality, cost, functionality, and availability of a UAV as "Cyber attacks on drones can pose significant safety risks to physical entities like large aircraft, airports, and human property. If compromised, drones can cause a larger impact than a regular IT device. As a result, UAVs require highly reliable software and strict regulatory compliance like the vehicle industry" [90]. And "Proactive prevention for public safety threats is one of the key areas with the vast potential of surveillance and monitoring drones. Antennas play a vital role in such applications to establish reliable communications in these scenarios. This paper considers line-of-sight and non-line-of-sight threat scenarios from the perspective of antennas and electromagnetic wave propagation" [91]. The development of directional and other types of UAV antennas has been discussed in the literature as in [92], [93], and [94].

In paper [95] they have proposed "a cyberspace security situation prediction model based on MapReduce and SVM (MR-SVM)". A performance assessment of various vulnerability scanners is reported in [96] and several types of vulnerabilities have been found by analysis using Nessus Scanner [96]. "GPS-dependent UAVs require accurate, trustworthy, and uninterrupted position information for their safe operation. However, different research efforts have shown that GPS signals can be jammed or spoofed owing to its inherent vulnerabilities" [98]. An analysis of the spoofing signal effect on a UAV receiver in a navigation spoofing experiment has been done by [99]. A well-designed system will take into consideration the deficiency of expertise on the customer side, however, it usually gets the least priority making many systems susceptible to attacks.

3.2. Suggested Solutions

The selection of the optimal UAV to perform specific tasks is not trivial, [100] have suggested a model that identifies UAV criteria and their weight using an analytical hierarchy process, then ranks each UAV using the technique for order preference by similarity to the ideal solution.

In this research, I have identified six main criteria that could enhance the cyber-physical security of perimeter UAVs which are ranked according to their level of security. The weight of each criterion will depend on the specifics of each task and its intersection with the other important considerations of performance level, cost level and overall system efficiency. "The process of evaluating alternatives is very complex and not well understood, and the information managed is incomplete, imprecise, and vague… A Hybrid Fuzzy-Weighted Average (HFWA) approach was proposed to offer an opportunity to carry out fuzzy analysis which takes full advantage of the information available to the decision maker” [101].

Considering the specific application of perimeter surveillance, the main criteria would differ from those of general cyber security, allowing to optimise the selection process of how to design each piece of hardware onboard within an acceptable trade-off with its functionality, while at the same time using its functionality to support the detection, identification, classification, management and prevention of cyber-physical security attacks [R1].

3.2.1. Supply Chain

Some incidents of pre-installed malware during the supply chain necessitate that the management of UAV cybersecurity starts by studying each stage of the supply chain. The UAV supply chain includes all the entities that work to make the product’s hardware, software, or service. Typically the supply chain is complex and dynamic consisting of tens of entities cooperating at some level to the final product, therefore, due diligence of checklist steps should be taken to satisfy the triad of confidentiality, integrity, and availability requirements. The testing includes an activity that might affect the final product regardless of the motive which could be due to,

- malicious;
- negligence;
- accidental.

The transparency of each entity in the supply chain about their security procedure to prevent flaw as well as their policy regarding reporting previous security incidents. The assessment of the UAV's immunity to cyber threats in the supply chain should be a deciding factor in its selection and purchase.

3.2.2. Antennas Radiation

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. Figure 12. shows the propagation of omnidirectional and directional antennas.

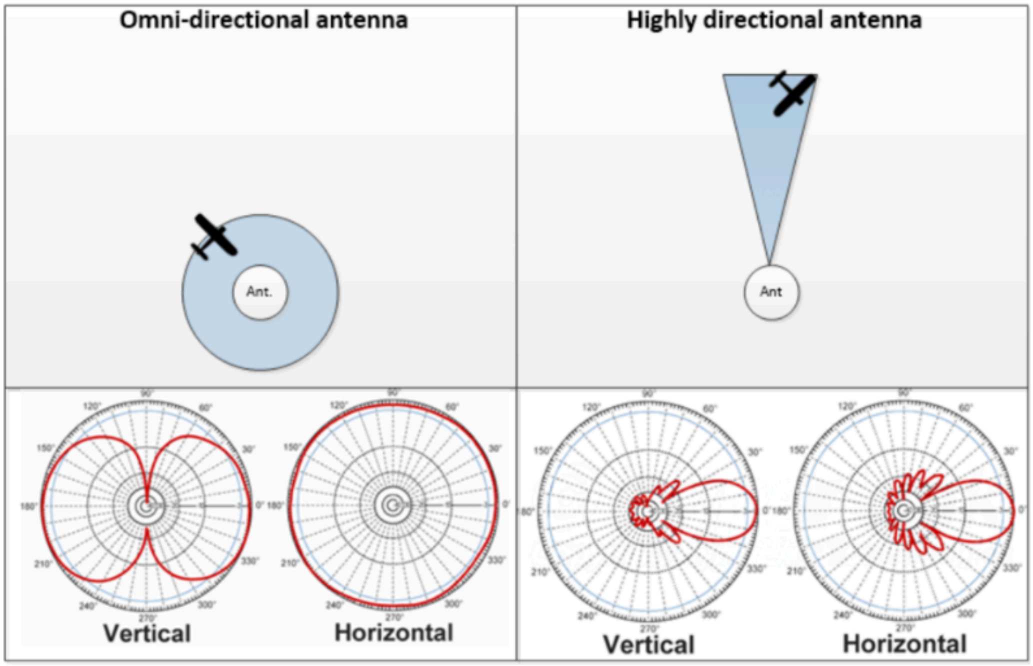


Figure 12. Omnidirectional vs directional antenna propagation [102]

The omnidirectional transceiving could be suitable in an emergency situations and not the default, steered transceiving can be controlled to a selected tolerance that is narrow enough to be secure and wide enough for flexible operation, the nature of operating surveillance UAV on a predetermined flight path facilitates steering both antennas propagation direction electronically, based on the planned flight path to ensure that the transmitted signal is only directed into the specific location of the targeted area, and the received signal is only possible to interfere from a specific location. Figure 13. shows patterns of electronically steered directional antennas simulated at different phases.

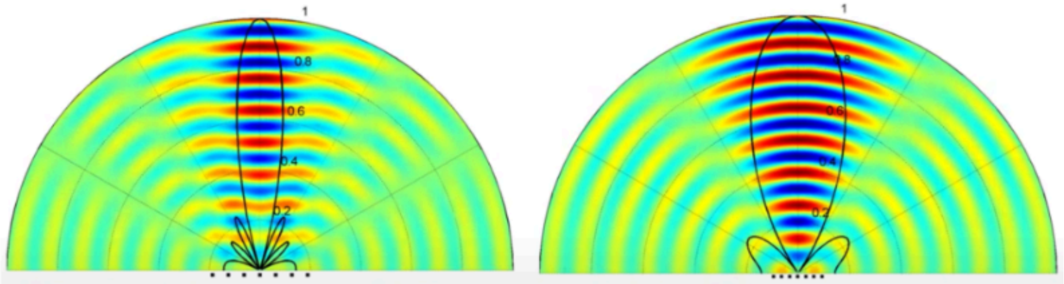


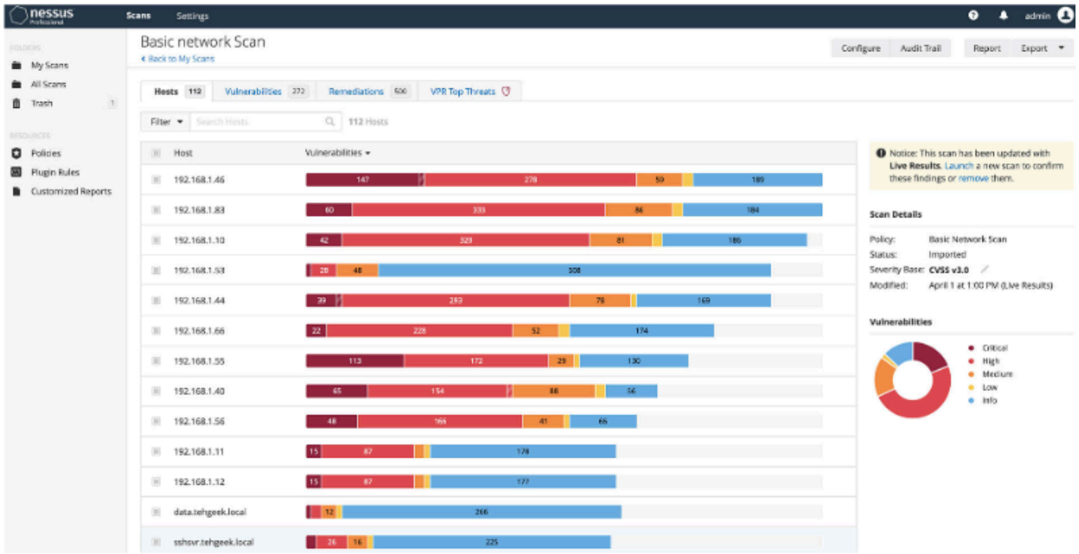
Figure 13. Propagation patterns of electronically steered directional antennas simulated at different phases [Author]

3.2.3. Network Mapping

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.

A 5G network provides an extended wireless connection to the internet, which exposes the UAV interconnectivity to a much wider range beyond the line of sight (BLoS) of the GCS, with a fraction of a second latency and a data rate of multiple gigabytes per second, however, keeping the network private would reap the benefits of the technology without high cybersecurity costs. The proximity of the surveillance UAV to the perimeter works well for the limited distance range of 5G, and the operating altitude would have few to no signal-impenetrable-obstacles.

An automated vulnerability scanner can highlight most of the critical attack points in the network [97], 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. Figure 14. shows an overview of a vulnerability scan report.



Basic network Scan
‹ Back to My Scans

112 Hosts

Host	Vulnerabilities
192.168.1.46	147 278 59 189
192.168.1.83	60 333 86 184
192.168.1.10	42 323 81 186
192.168.1.53	28 48 508
192.168.1.44	39 283 78 169
192.168.1.66	22 228 52 174
192.168.1.55	113 172 29 130
192.168.1.40	65 154 88 56
192.168.1.56	48 165 41 66
192.168.1.11	15 87 178
192.168.1.12	15 87 177
data.tehgeek.local	12 266
sshsvr.tehgeek.local	26 16 225

Notice: This scan has been updated with **Live Results**. Launch a new scan to confirm these findings or remove them.

Scan Details

Policy: Basic Network Scan
Status: Imported
Severity Base: **CVSS v3.0**
Modified: April 1 at 1:00 PM (Live Results)

Vulnerabilities

Figure 14. An overview of the Nessus vulnerability scan report [103]

3.2.4. Navigation System

Global Positioning System (GPS) is the most widely used system for navigation, GPS spoofing is an attack that denies or distorts the GPS signal. Although a large number of countermeasures methods have been published for UAV navigation system spoofing attacks, and many are implemented by manufacturers, this type of attack is still reported. A combination of several computationally efficient methods could reduce the susceptibility to spoofing. Onboard positioning of the UAV using multiple techniques and comparing them would help to create a voting mechanism to determine the true position at all times:

- positioning based on GPS;
- positioning based on inertial measurement unit IMU;
- positioning based on machine vision;
- implementing a geo-fence (whenever it limits exposure to spoofed signals).

3.2.5. Encryption

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. [104] concluded that "general IT cryptography cannot meet all UAS requirements".

For filtering noise, "simpler and primitive heuristic methods that are not related to the concept of optimization for special noise distribution can provide acceptable results for filtering noisy signals in the fixed point iteration-based adaptive control. As the less complicated and less computational power-greedy solution the use of a simple low pass filter with Euler integration can be recommended" [R5].

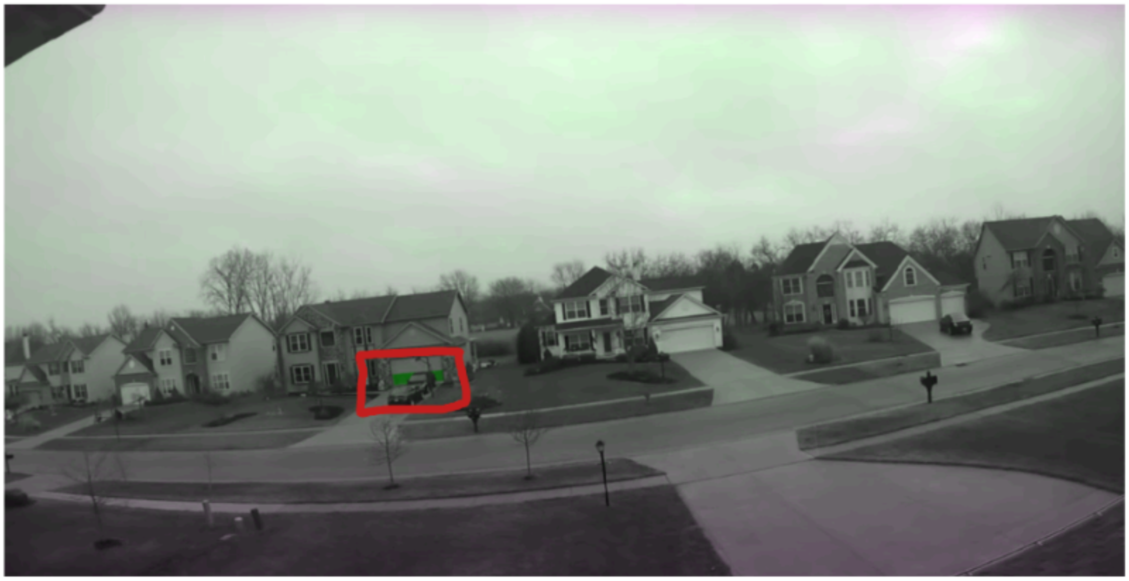
3.2.6. Machine Learning

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. An example of a surveillance sign identified by the model. Figure 15. shows a sign of a previous activity detected by a machine learning model.

(A)

(B)



(C)

Figure 15. (A) shows the first surveilled scene, (B) shows the same location after time interruption, (C) shows the machine model identifying the highest difference between (A) & (B). Highlighting a sign of a potential suspicious event, in this case, the highlighted garage door was opened during the absence of the surveillance UAV [105], processed by author

3.3. GPS\GNSS Spoofing

This section discusses the vulnerability of UAVs used for perimeter surveillance to GPS spoofing threats and discusses some approaches to manage them, reviewing complementary positioning methods using onboard IMU and camera sensors, and local positioning systems to increase the overall positioning accuracy and decrease the dependency on GPS. The vulnerable, weak, and unauthenticated GPS signal necessitates techniques to handle the worst-case scenarios independent of GPS.

GPS spoofing is of great interest to the UAV cyber-physical security community. UAVs have proliferated in many sectors ranging from less sensitive applications to more sensitive ones such as surveillance. The vulnerability of UAVs to cyber threats is similar to that of any computing device like a smartphone or a modern internet-connected car. However, GPS spoofing could result in an attacker gaining access to the physical UAV, flying it to attack people or damaging physical equipment. Relying on a large corporation to provide the immune system with regular updates can prioritise high security. However, this dependency often leads to issues such as monopolisation by a single service provider, rather than integrating multiple navigation sources like BeiDou, Galileo, and GPS.

Investigations of previous attacks may create a false sense of security. This biassed perception can be linked to aeroplane crash investigations, which often lead to robust and, in many cases, lasting solutions. However, spoofing poses a different challenge; it is unlikely to have a permanent solution, as advanced systems continue to experience failures.

Recent incidents highlight this issue. For example, during the 2017 Black Sea attack, the location of an on-land airport was transmitted, causing some ships to receive false information about their current positions. In 2023, a Boeing aircraft was likely spoofed over Cairo airspace, leading aviation authorities to mistakenly believe it was stationary for 30 minutes. That same year, fake navigation signals were also detected, underscoring the ongoing vulnerabilities in aviation security.

GPS signals received near the earth's surface are considered unauthenticated and weak (around –155dbW). Easily generated signals at a similar frequency but higher power would overwrite them, enabling a low-cost attack point, especially on an UAV which is exposed by nature of the operation. The limited onboard capacity in terms of payload, computing power, memory, and energy consumption, forces the decision makers to find new ways to compensate for the deficiency of onboard cyber defence hardware and software by installing alternatives in the GCS and achieve a cost-efficient solution that satisfies standard security requirements. Figure 16. shows an illustration of a spoofing attack.

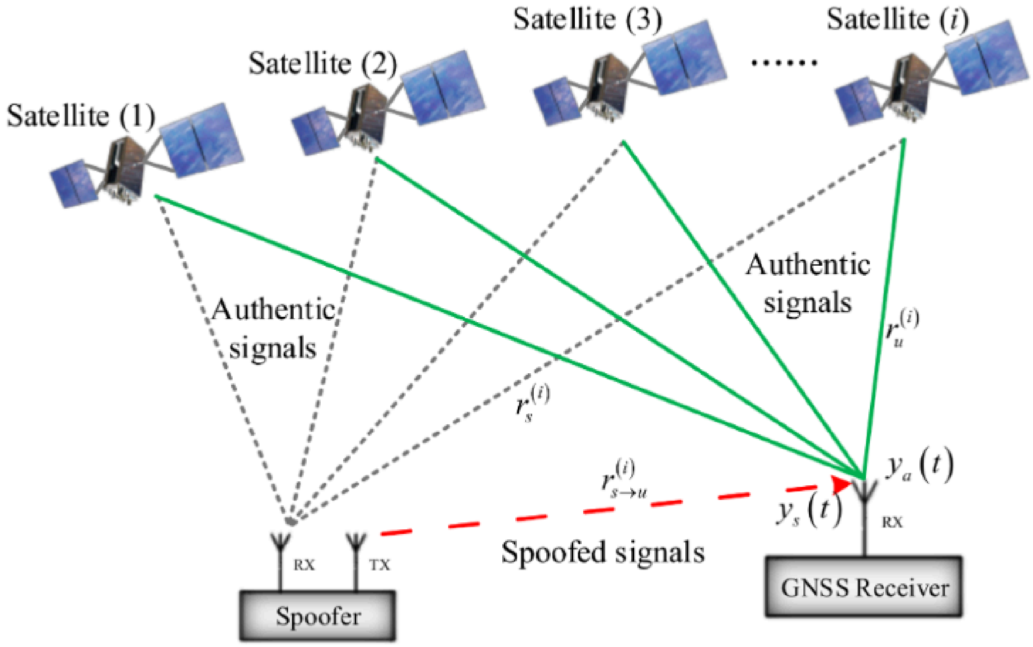


Figure 16. Signals spoofing attack illustration [106]

The three main levels of securing the UAV against spoofing are prevention, detection, and mitigation. A total dependency on one positioning method exposes the system to higher risk, the onboard receiver is the first line of defence, and one or more differences between the GPS and the spoofed signal can be detected and then acted upon by the receiver discrepancies such as the signal timing, direction, strength, and noise ratio are among the detectable anomalies identified in the literature.

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 as described in the next section.

3.4. Complementary Positioning Methods

3.4.1. Positioning Based on Inertial Measurement Unit (IMU)

This method is independent of wireless control signals and requires no additional onboard hardware, the IMU is an accelerometer that measures the linear acceleration of the UAV and a gyro sensor to measure its rotation in the 3-dimensional space, and many IMU units include a magnetometer. The processor can estimate the real-time position in reference to the launch platform by accumulating the sum of distance and direction data with relatively poor accuracy (metres), fusing other sensor data and using software techniques such as the Kalman filter to improve the accuracy. The main disadvantage of this method is the cumulative error, therefore, it's mostly used simultaneously with other methods, its low requirement of computation power and no additional hardware attract the designer to include it with various positioning techniques, an example of an integration mechanism of two positioning methods is shown in Figure 17.

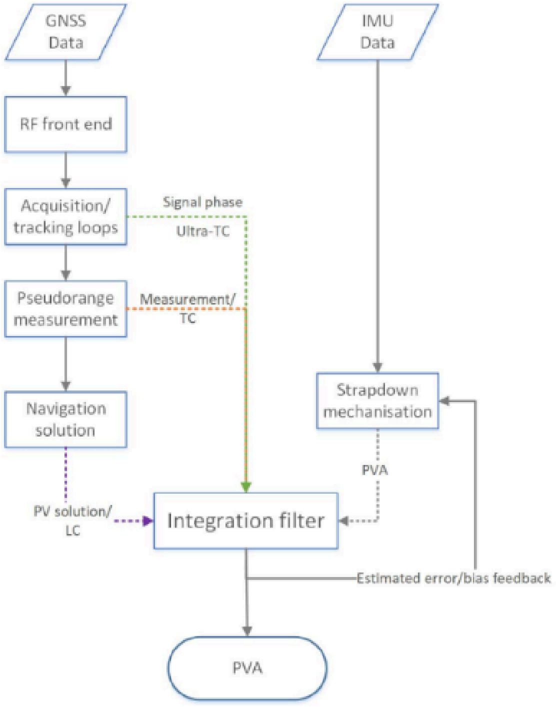


Figure 17. The integration mechanism of two positioning methods, measuring the time of arrival of the GNSS signals via the Timing Channel (TC) and the phase of the signal through the L1-signal Carrier (LC) to determine position, velocity, and attitude (PVA) [107]

3.4.2. Local Positioning System (LPS)

The Local Positioning System uses 3 or more ground-based radio signals, which are often used as an alternative or complement to the GPS satellites, developed mainly for indoor and in areas where the GPS signal is weak, the concept could be used to provide limits to the flight path that protect the UAV from being spoofed away but not necessarily provide a precise position, a fully integrated network of sensors and beacons positioned on the ground environment along the UAVs path can provide a precise position but it would be an additional cost with small security leverage.

Unlike GPS signals, LPS signals can be authenticated and encrypted reducing the probability of spoofing attacks, however, this is a high cost, high complexity solution, and only suitable for a dedicated purpose infrastructure. The accuracy is relatively good especially when combined with another method, and it works in all weather conditions, day and night. The current rate improvement in electronic performance in parallel with reduction of cost have increased the feasibility and effectiveness of such methods in some critical infrastructures. Different approaches have been suggested in the literature reviewed as the follows,

- measure the signal attenuation to estimate the travelled distance from the transmission point;
- measure the angle of the received signal to estimate the orientation of the transmission point;
- measure the time delay of a clocked signal from different transmission points.

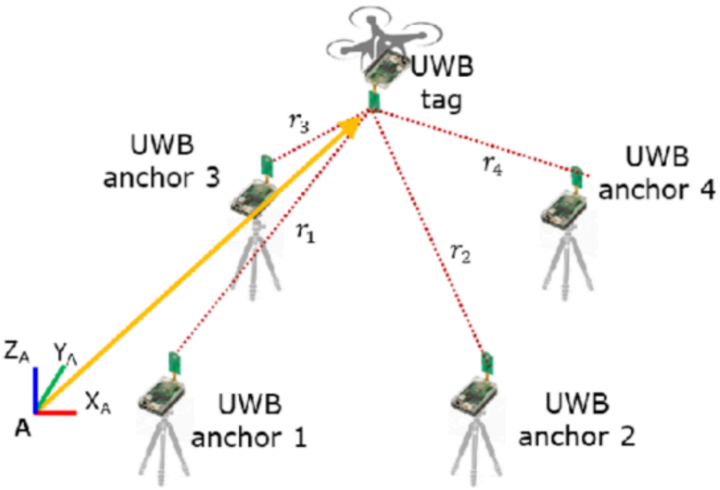


Figure 18. Illustration of Ultra-Wideband (UWB) ranging positioning system [108]

The inherited complexity of real-life application vs a controlled environment makes the risk of signal reflection a major drawback of the method and limits its usability in specific operation sites. The main advantage of this method is that the energy and computation consumption are mostly on the ground stations not onboard the UAV.

3.4.3. Positioning Based on Vision

This method uses known visual ground cues to estimate the UAV position, and it achieves high positioning accuracy, the main disadvantages come from higher consumption of onboard computing power but still feasible, and low effective when operating in low visibility environment, many algorithms for navigational aid and estimator of distance to approaching obstacles could be implemented, and the camera is standard hardware on the UAV, to operate during low visibility thermal camera or radar have been reviewed in the literature with effective performance. The optimisation of a shortest path that is suitable to navigate through some limited visibility requirements, has been researched extensively in the field of computational geometry, known as the “Watchman Routing Problem” [109].

Surveillance UAVs are mainly tasked to collect and analyse visual data, an onboard model that integrates image light intensity with accurate time and location of each image frame is an essential key performance of the system, although computational consuming, vision positioning by feature matching is an accurate, reliable, and cost-effective solution that has the characteristics to override all other methods in an autonomous mode.

3.4.4. Positioning based on other sensors

LiDAR uses laser pulses to estimate the distance to the ground objects by measuring the time it takes for the reflected pulses to return to the receiver. In addition to all the limitations of vision, LiDAR is limited in range, and expensive (not a standard UAV sensor). The arguably higher accuracy has no added value over the vision method accuracy to countermeasure a spoofing attack. Acoustic sensors have similar range limitations.

In practice, the challenge arises for navigation priority in case of mismatched positioning, assigning a voting power is sufficient in a specific scenario, but should be abruptly changed according to the overall situation, accurate collision avoidance and potential landing site detection still has many challenges in real life scenarios, computer vision is a domain that has the potential to satisfy multiple UAV system robustness requirements, it's a cost-effective in terms of hardware, software and onboard resource consumption.

The environment in which the UAV operates can affect the overall reliability, the IMU is susceptible to a drift error, which can accumulate over time, and blur and low visibility conditions affect vision performance. Any change in the operating environment will dynamically change the reliability of certain sensors, therefore human supervision is still needed.

Positioning is the cornerstone for autonomous navigation, GPS spoofing is a potential cyber-physical threat mostly for poorly designed systems, and many effective techniques could be implemented to mitigate the consequences of the attack, positioning based on multiple methods is feasible, and optimal to negate the disadvantage of individual methods, a combination of inertial and visual positioning can aid by improving accuracy and providing redundancy, autonomous flight systems are not fully mature for the majority of locations.

3.5. Physical threat protection

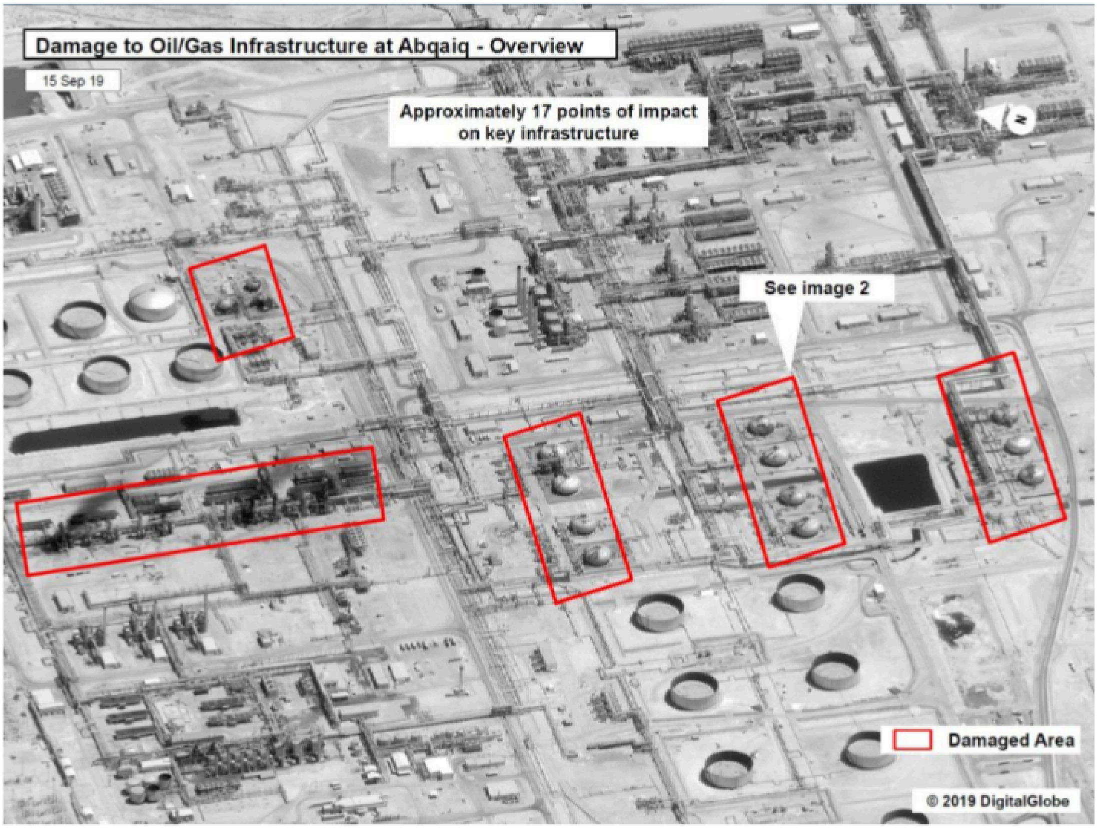
Dealing with external threats is one of the highest priorities when it comes to securing critical infrastructure. Protecting such facilities requires continuous adaptability. The proliferation of drone technology accentuates a new threat, the low cost and ease of access makes it an effective weapon that poses a great danger to most facilities. In this section we will discuss the need for a slat armour to protect from aerial objects, the traditional fences protect against objects at ground level only. an overhead slat armour is necessary to protect against flying objects and drone intrusion.

Until recent years, building a regular fence around the perimeter of critical facilities was considered enough to comply with regulations. Most vulnerability and risk assessments had assumed a low risk of airborne intrusion. Flying objects (either birds, objects carried by wind, or vehicles) were considered to be a lower risk than ground intrusion, therefore, no physical barriers were required to protect the overhead space.

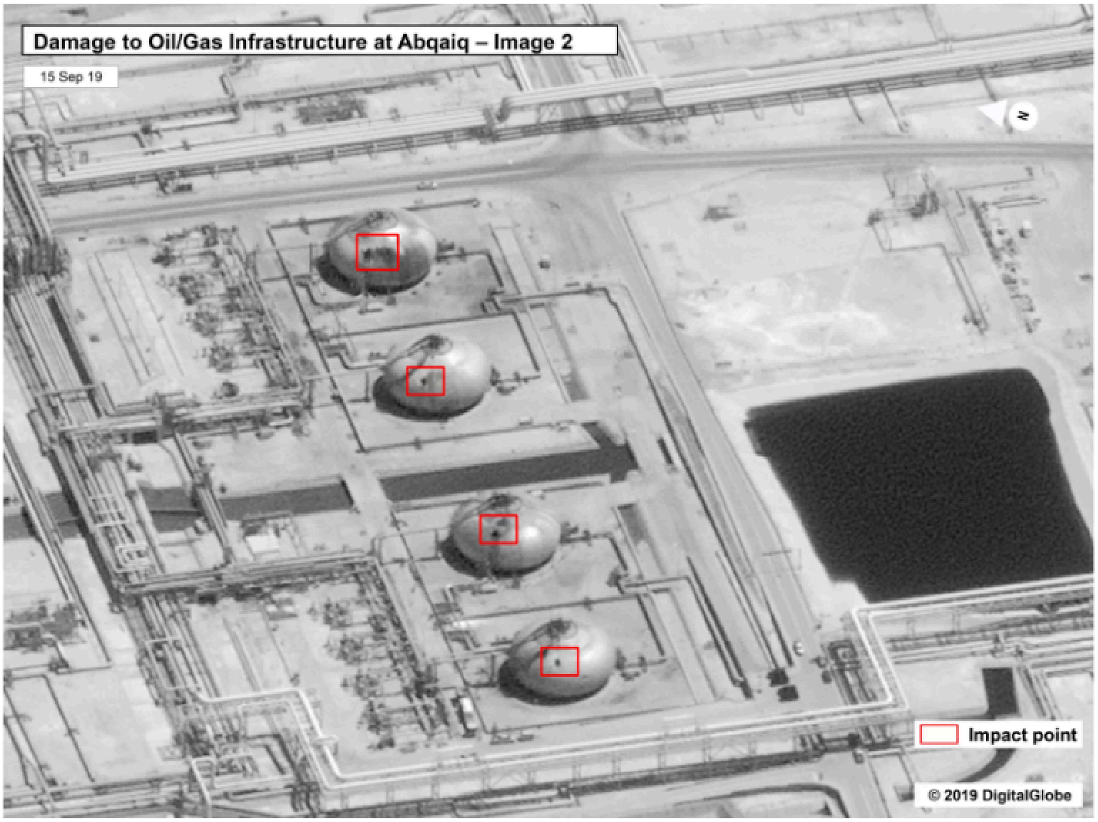
Traditionally, a state that had the capability of conducting an intentional aerial attack was deterred by the risk of open war. and a high-tech defence system is much more effective than physical armour. For some facilities such as military air bases the risk/reward assessment favours three dimensionally reinforced hangars to shelter military aircraft.

In recent years the world has witnessed a proliferation of UAVs. It is affordable and easy to access and able to carry multiple kilograms of explosives for many kilometres and hit a target accurately. These capabilities are now available to individuals who can use them to access equipment, installations, and materials causing sabotage, damage, or theft. A physical fence against UAVs is an important part and serves as a last line of defence together with other elements and components.

In September 2019, an attack on the world’s largest oil processing facilities showed the danger of drones penetrating critical infrastructure. The missile defence system failed to stop the swarm of drones and cruise missiles that struck the oil infrastructure. Figure 19. shows some of the physical damage caused by the attack.


Damage to Oil/Gas Infrastructure at Abqaiq - Overview
15 Sep 19
Approximately 17 points of impact on key infrastructure
N
See image 2
🟥 Damaged Area
© 2019 DigitalGlobe

(A)



(B)

Figure 19. An aerial photo showing some of the damages on the oil processing facility [110]

Many unique offensive advantages of drones could be reduced by an overhead slat armour, the small size which makes a drone less visible to radars means a small mass of explosives, and the low flight altitude will result a less kinetic energy impact, similar thing with the high manoeuvrability which means lower speed and therefore less kinetic energy impact. Similarly to the API Std 650 standard published by the American Petroleum Institute (API), the European standard EN 14015 code for oil storage tank shell's thickness doesn't take into the equation any external up-normal impact as we can see in the equation used to calculate the outer shell thickness shown here:

$$e = \frac{D}{20S}\left(98W(H_c - 0.3) + p + c\right)$$

Where:

c -is the corrosion allowance in [mm].

D -is the tank diameter in [m].

e -is the required thickness in [mm].

Hc -is the distance from the bottom of the shell course [mm].

P -is the design pressure at the top of the tank in [mbar].

S -is the allowable stress for the appropriate condition in [N/mm2].

W -is the density of the liquid under consideration in [kg/l].

For the shielded spherical-shaped tanks we can see that although the impacts have created holes and started a fire, the explosion was not strong enough to destroy the tanks. For decades fences have been rated by performing the fence crash test, where different types of vehicles crash into the fence at different weights and speeds [R3]. The fences are usually rated based on how far past the fence the vehicle travels in each scenario. Figure 20. illustrate the crash testing.

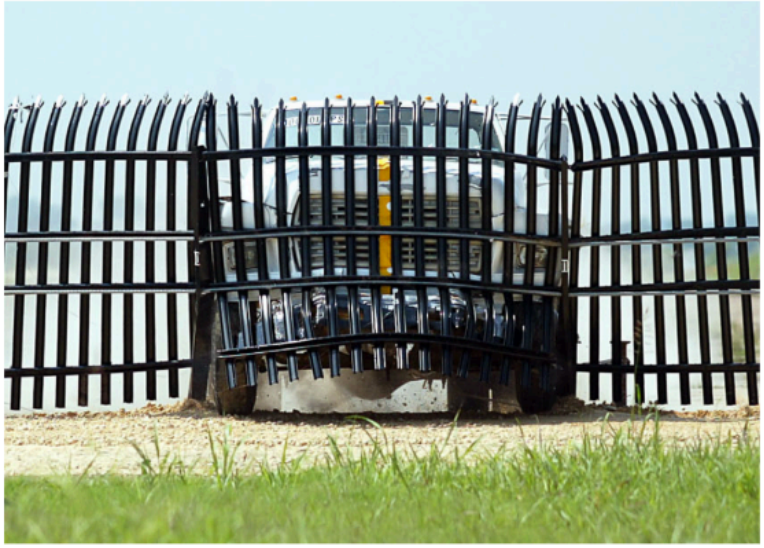


Figure 20. An illustration of a crash test for fence rating [111]

The American Society for Testing and Materials (ASTM) has developed crash certifications for different types of vehicles. They are as follows:

- C -ratings: small passenger car (2430 lb.)
- PU -ratings: pickup truck (5070 lb.)
- M -ratings: medium-duty truck (15,000 lb.)
- H -ratings: heavy goods vehicle (65,000 lb.)

A similar rating could be applied to different types of slat armour. A similar rating to certify different types of slat armour against aerial objects will help designers and security officials consider the feasibility of integrating the armour into the facility relatively small, the additional costs, weight, and space required will be evaluated with a vulnerability and risk assessments and how it can affect the insurance policy of each facility [R3].

Aerial objects could be classified based on whether the object is loaded with specific weapons (explosives, firearms, chemicals... etc.). Most of the drones (including the ones used in the Abqaiq attack) that can be acquired by individuals or groups weigh less than 150 kg (nearly half of it a payload), with a maximum speed of 500 km/h and a maximum altitude of 4 km, providing them limited kinetic energy. Together with other security systems elements and components an overhead slat armour can be very effective for this specific threat, the cost, weight, and space of such construction would allow for a multiple layer to stop these drones or detonate the explosives before reaching their targets, therefore, reducing the overall impact.

The rapid advancement and affordability of UAVs are likely to increase their use in criminal activities, especially for bypassing security fences. While air defence systems can effectively protect no-fly zones, a careful assessment of the benefits-to-cost ratio is essential. This includes comparing the cost and protection level of slat armour with the expenses of air defence systems and the economic repercussions of flight prohibitions. Such analysis is vital for protecting critical infrastructure and may necessitate a combination of both measures in scenarios involving indiscriminate risk.

3.6. Conclusion

The focus of this chapter is to identify the main criteria to achieve adequate cyber-physical security levels for surveillance UAVs despite the exposed nature of the operation and the limitation of onboard resources capacity, whenever possible the defensive tools should be installed in the ground stations.

1. We found that using directional antennas could improve power consumption, increase the signal range, and reduce the attack space on the communication line significantly.
2. WPA3 encryption is effective for ground stations, lighter encryption for onboard use such as Bleep64 would save onboard resources.
3. Machine learning models have already achieved a high level of performance in analysing big data to predict and prevent cyber attacks, as well as increase the performance efficiency of the system.
4. The main limitations are the high cost of solutions and complexity, as cybercriminal threats are inventive and innovative with new strategies and techniques.

From a cyber-physical point of view, a few incidents of advanced UAVs have been spoofed or gunned down during surveillance, raising the risk concerns of both economic and more importantly the information cost. However, for a security technology the current security measures are considered to be sufficient enough for the predefined level of security, with no evidence of substantial extra risk from the use of perimeter surveillance UAVs, and compared to other security technologies the author finds recent advancements are enough to provide an adequate cyber-physical security level, supporting **Hypothesis 1** 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” and supporting **Hypothesis 2** 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”.

4. 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.

In the Large-Scale Visual Recognition Challenge 2015 (ILSVRC2015) a trained artificial neural network “ResNet” had better results than human experts, and since then computer vision has even improved in terms of speed and accuracy, therefore it has been deployed in many industries and applications most famously in autonomous cars.

The cornerstone of man-tracking is to find the signs, which are the physical evidence of any disturbance of the environment left behind by animals, humans, or objects. The search for this sign is called sign cutting. A person (or animal) cannot traverse the ground without leaving some sort of telltale sign. This sign is what we’re trying to find and track in video footage/images using computer vision [R4].

Large region continuous surveillance is usually cost-prohibitive, leaving the periodic surveillance the only viable option for the majority segments of the surveilled region. The analysis of the collected data should include a search for clues about events that occurred during the unsurveilled period. One way to increase the effectiveness of finding those clues is by performing image registration to highlight the disturbances of the environment that might contain signs of certain events. This chapter discusses the possibilities and limitations of applying image registration techniques in sign cutting to the data collected by surveillance unmanned aerial vehicles and shows some detected signs in surveillance imagery by an automated image registration model.

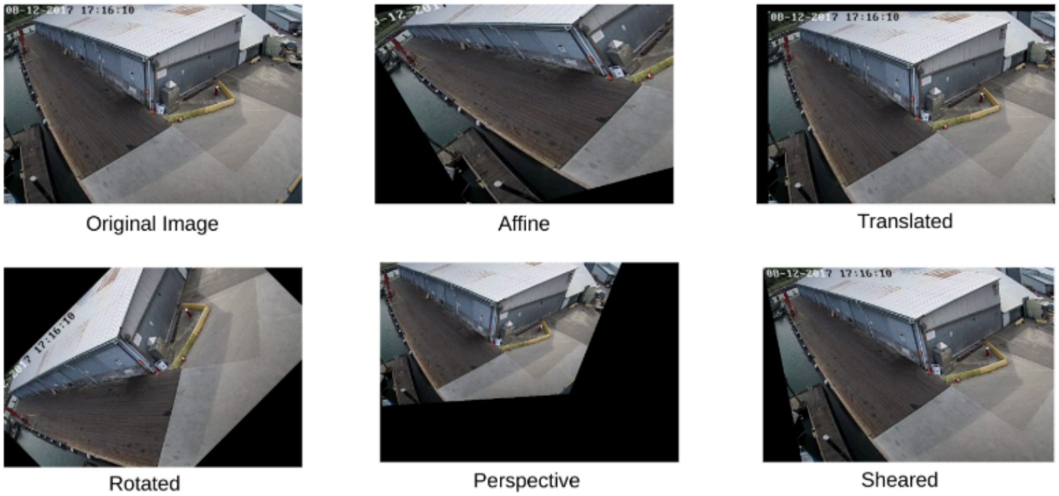
4.1. The Challenge

The security challenges for the 21st century are immense, according to the United Nations Office on Drugs and Crime in 2009, transnational organised crime was estimated to generate $870 billion — an amount equal to 1.5% of global GDP [112]. That is more than six times the amount of official development assistance for that year, and the equivalent of close to 7% of the world's exports of merchandise. The gangs are growing bigger and getting more sophisticated, and as any other business, they are in continuous efforts to expand.

Trespassing of an individual is relatively easier than before due to advances in smartphones, global positioning systems, electronic maps, and weather forecasts which enabled an average person to cross transnational borders from terrains traditionally considered as hard to cross e.g. (deserts, jungles, and heights, etc.). The need for reliable and efficient solutions is urgent, and it has become a mainstream debate for many policy makers.

Millions of sensitive kilometres around the world are left unfully surveilled due to high cost, resulting in numerous breaches, and large stretches of energy pipelines are getting attacked and vandalised, [113] studied the global consequences of oil theft, he estimated that the total losses reached USD 133 billion, which equate to 5–7% of the global crude and refined petroleum market, and give criminal groups large amount of financial resources to be used in other criminal activities that affect and claim many lives. UAVs have been utilised in many industries, providing reliable and cost-effective solutions. Surveillance UAV covers a wide spectrum of capabilities, one surveillance UAV carrying a camera could fly daily to collect imagery of oil pipes that stretch hundreds of kilometres.. This type of minimal surveillance, although limited to one scan per day, could provide significant security benefits, and require analysis to extract the most high-quality information out of the collected data. The image registration process could be automated to highlight some segments of the surveillance area that need the highest attention and further investigation by detecting areas with the most clues of disturbance and change [R4].

To overcome the variation of image field view, a geometric transformation is needed. The procedure starts with selecting some common features in the images, each matching feature will be considered as a control point, then a final transformation of the control points is shifted using an estimated matrix function to align the images group. The following Figure 21. shows some transformed images from the original scene.



Original Image

Affine

Translated

Rotated

Perspective

Sheared

Figure 21. Shows some transformed images from the original scene [114], the rest of the images are processed by the author

This process is cost-prohibitive, especially for a large amount of imagery, therefore, it should be automated by selecting specific parameters from each registration type, the application will determine the fine-tuning of the procedure to maximise the overall precision.

Besides cameras, surveillance UAVs could be equipped with many other sensors. Chemical sensing UAV is emerging in agriculture and air quality applications and can play an important role in the surveillance of critical infrastructures by detecting and localising foreign scents. The Airborne Ultra-light Spectrometer for Environmental Application (AUSEA), is a project initiated by Total Group in partnership with France’s National Center for Scientific Research (CNRS). AUSEA is a miniaturised gases sensor, fitted onto a commercial UAV and used by Total Group [115], scents can be from various sources, and some volatile organic compounds have resulted from bruised vegetation, hormones, and pheromones produced by insects [116].

Chemical sensing UAVs are a rapidly emerging technology and have more limitations than visual imagery, the main limitations are the concentration of specific gases in an open environment, the time & effort needed to localise the source of these gases, and the sensor sampling method, the air sample must be taken from the least disturbed space, the main disturbance is caused by the airflow generated by the propellers of the UAV, to avoid any impairment of the measurement results and maximise uniform sampling. [117] has calculated the aerodynamics of multi-rotor UAVs, similar studies are important to design the optimum sample intake for a chemical sensing UAV. Figure 22. shows the velocity vectors and static pressure values on a multirotor UAV body.

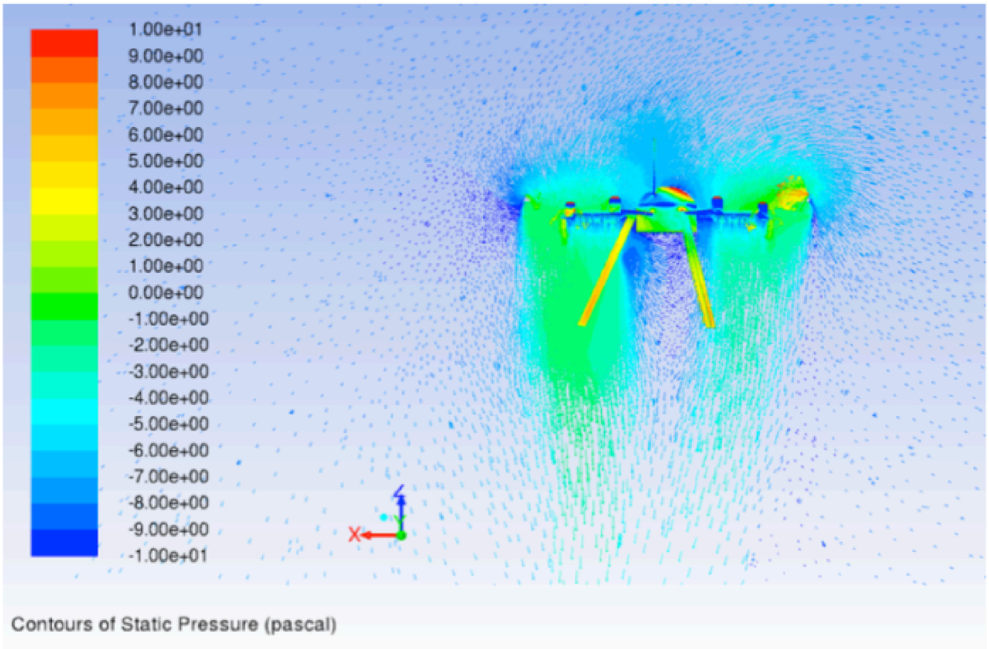


Figure 22. Velocity vectors and static pressure values on a multirotor UAV body [117]

4.2. The Limitation

The practical operation of surveillance UAVs requires maximum flexibility in terms of some updating on the flight path, and requires precise positioning and high position repeatability. [79] described a 3D flight path planning for multirotor UAVs emphasising solutions for the UAV take-off and UAV landing. In [118] terrain-following missions for low-altitude UAV flight path planning are described. “Image registration has supported UAV landing on a runway” [119], as well as UAV localisation [120]. Some localisation of geometric differences techniques have been described in [121], [122].

[123] Investigated the airflow pattern caused by the multirotor UAV, Figure 23. shows the airflow pattern caused by the multirotor UAV (DJI S900) using three coloured pyrotechnical smoke cartridges with (a) flying the multirotor UAV below the lowest smoke plume, and (b) below the middle smoke plume; Side wind from right to left. Dilution of the smoke plume and thus mixing of the surrounding air occurs essentially only on the lee side and below the multicopter UAV, while in windward and above the multicopter UAV, the approaching plume remains largely unaffected.

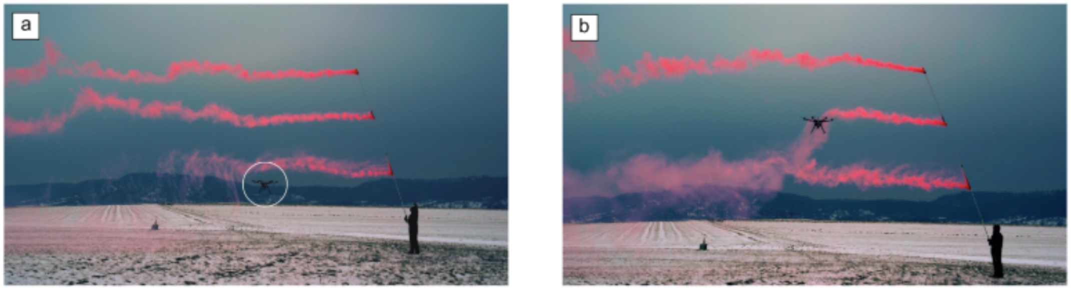


Figure 23. Distorted airflow caused by the multirotor UAV and its effect on the gas plumes [123]

Both the wind and the UAV downwash affect the air sample. Using metal oxide semiconductor (MOX) gas sensors, some attempts have proved the concept such as [124] and [125], although both attempts have many limitations of needing a high external computing power, limited mapped space, and accurate external positioning for the UAV.

One significant practical detection of a person to rescue him is reported by [126] that studied a real-life human rescue using an automated Search and Rescue with UAV software that used an external laptop to analyse 782 JPG images, successfully locating the person in a few hours. The regulations regarding surveillance UAVs are behind the state of the art of the field, slowing down practical demonstrations of new technologies and techniques, [127] report on the lack of defined norms, stating what to be done in the future to fill gaps, create missing regulations. The magnitude of areas to be monitored as a potential crossing point is huge which requires an overwhelming number of manpower of human analysts. Besides finite resources & insufficient manpower, poor training, inadequate surveillance equipment, and corruption make the task much more difficult.

The varieties of critical infrastructure laws and regulations demand a flexible security system, many of the energy pipes are near the ground surface and subject to theft or sabotage on a daily basis. Monitoring such lengthy stretches of terrain requires reviewing millions of images and hours of video footage daily, which is inefficient and practically impossible to accomplish by manpower alone.

UAVs could fill a gap in the current lengthy border surveillance by improving coverage along remote sections of the borders. Moreover, the flight distance range of UAVs is a significant asset when compared to border agents on patrol or stationary surveillance equipment. One of the most important questions of UAV flight is the real-time flight path design. The upgrade from manual UAVs flying by an operator to an autonomous flight substantially reduced the operating cost. Some new software optimised the auto-pilot flight path by visually detecting a certain moving object (moving target indicator) and following it. However, to cover a lengthy path the surveillance UAV would have only one or few flights over a certain area per day, leaving the area un-surveilled for the rest of the day. To increase efficiency, we propose using visual recognition to detect the signs left by a trespasser e.g. (footprint, tire impressions, kicked-over rocks, soil depressions, changes in vegetation...etc.)

In 2010 [128] indicated that "the cost comparison between UAVs and manned aircraft is complicated. UAVs are cheaper to procure than manned aircraft but may cost more to operate. Thus, the life cycle cost of UAVs could be greater than the life cycle cost of manned aircraft. The disparity in operating the two types of aircraft may be offset by the fact that UAVs can remain in the air more than 10 times longer than the helicopters currently being used by Air & Marine (A&M) to support the US Border Patrol (USBP). Further, UAV command and control systems are being developed that can control multiple UAVs simultaneously. When fielded, these new capabilities may change the cost comparison to favour UAVs over manned aircraft". Since then the UAVs overall cost is getting down and they have already become the optimum option for certain cases cost-wise.

4.3. The Proposed Approach

The surveillance UAVs are usually equipped with one or a combination of normal camera, an EO camera, Forward Looking Infrared Radar (FLIR), a multi-spectral camera, and a Synthetic Aperture Radar (SAR).

The first step would be using Convolutional Neural Networks (CNN) to detect the signs from the video footage. CNNs such as GooglNet, Inception...etc. have shown excellent recognition capabilities, and these CNNs could be retrained to detect the signs of our interest (footprint, tire impression…etc.) and upon that, we can optimise the flight path accordingly. Figure 24. shows a tire impression near the US-Mexico border, in this case, if the impression was detected by the UAV during the routine surveillance flight, the autopilot would adjust the flight path and make an extra tour in the area within predetermined limits to collect more data which may lead to the intruder, and at the same time signals the border agents for further tracking actions. Flight altitude and the camera resolution would affect the detectable object size. A large benchmark dataset is needed to train and test algorithms and provide metrics such as the top 5 accuracy and error rates of different algorithms.

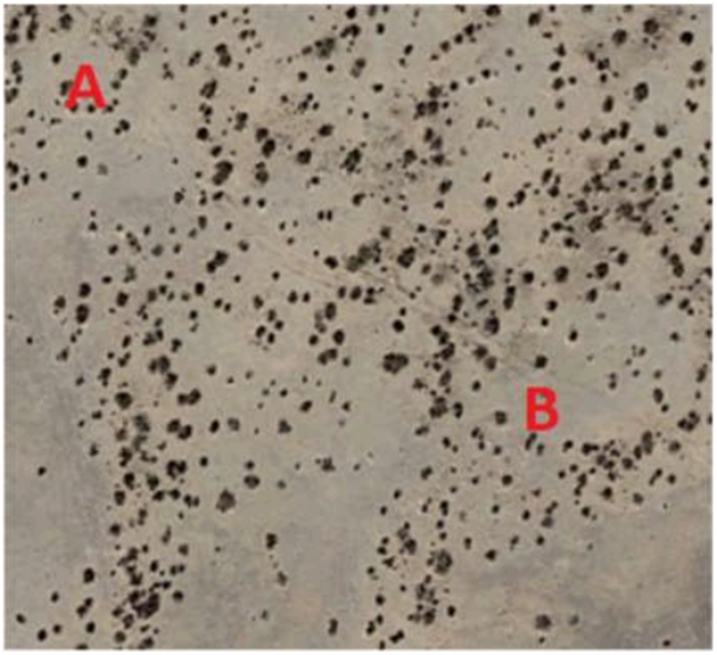


Figure 24. Tire impression near the US-Mexico border [Author]

For the best performance, the training dataset should consider the flight altitude, different soil types, and changes in weather. Another difficult factor is to estimate the age of the impression, it could be done by comparing the current footage with an older one to verify if the impression is new or not. It’s also important to consider that some impressions could be caused by the border patrol vehicles. Using special cameras could help find some other signs for example using FLIR cameras we detect thermal signs. One of the most detectable signs is the shadows made by our target object, even if the object had left the area before recording the surveillance video. Its thermal sign could be detectable. Figure 25. is an FLIR image taken by Global-Hawk UAV, the thermal shadows of aeroplanes and cars are still detectable even after the cars have been already left. CNN can recognise this kind of thermal shadow as well [R4].

The use of small drones to smuggle drugs and weapons across the border has been reported, canons as well used to shoot drugs packages across the border for an accomplice on the other side. Such a smuggling operation includes a criminal member to monitor the surroundings and provide an early warning to the other members that a surveillance UAV has been detected, therefore they could hide just before the area being surveilled. Having a computerised way to detect thermal signs would lead to a stop or even apprehension.

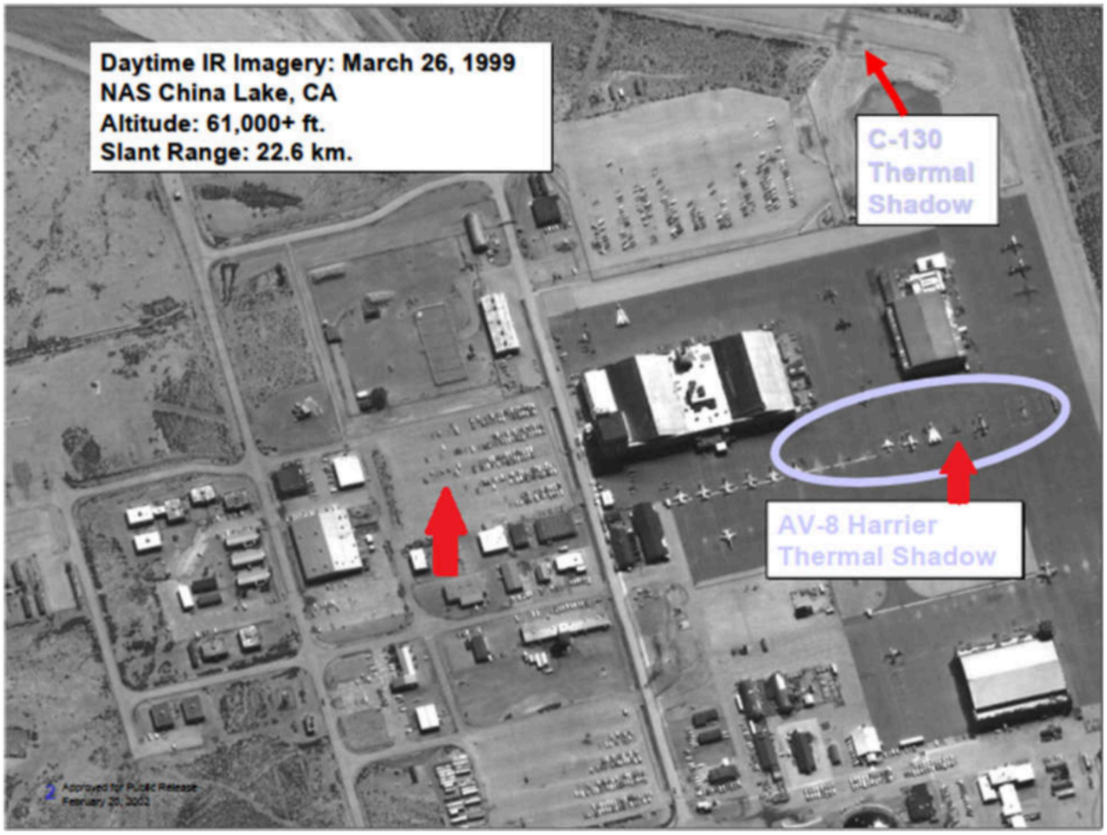


Figure 25. The thermal shadows [R4]

4.4. Signs to look for

The summary of all events that happened in a certain region of the border within the periodic surveillance time is represented in signs left behind these events. These signs could be physical or chemical, requiring different types of sensors to detect them. Any change in the environment of that region resulting from human, animal, object, or natural phenomena would be of interest, and the computerised model task is to help find these signs.

A. Physical signs

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% [129], 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 26.

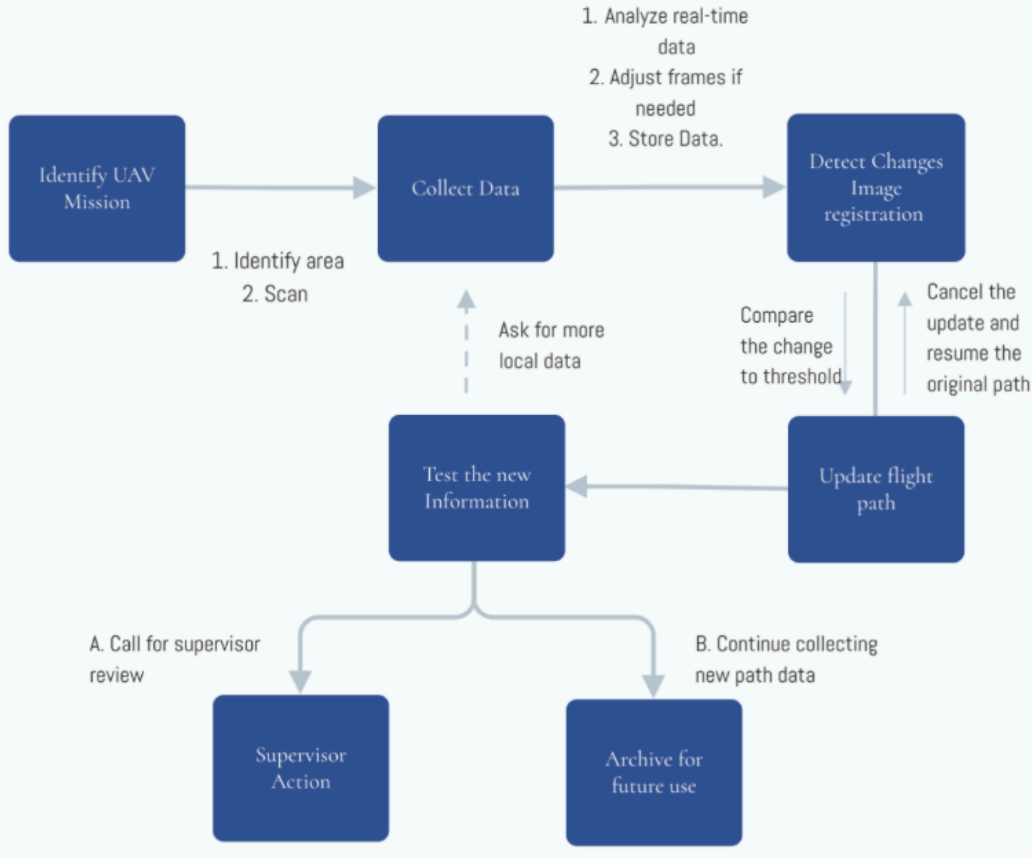

1. Analyze real-time data
2. Adjust frames if needed
3. Store Data.
Identify UAV Mission
Collect Data
Detect Changes Image registration
1. Identify area
2. Scan
Ask for more local data
Compare the change to threshold
Cancel the update and resume the original path
Test the new Information
Update flight path
A. Call for supervisor review
B. Continue collecting new path data
Supervisor Action
Archive for future use

Figure 26. Flowchart illustration of a scanning mission [Author]

Physical signs detected by analysing the image data are the main surveillance objective, as image analysis is a well-studied and mature concept that has accumulated knowledge for over a hundred years. Another important emerging sensor is electronic chemical sensing, despite being relatively at its experimentation phase, the data collected by the current sensors shows potential to improve surveillance.

B. Chemical signs

The movement of vehicles or living creatures across a region would probably leave distinctive chemical residues that are foreign to that environment. The exhaust gases of internal combustion engines, spelled out fuel and fluids, and cooking and human odours are chemical signs that are usually detected by trained dogs and could be detectable by UAV's sensors, however, trained dogs, while often used for detection purposes, are not always scientifically precise in their identification processes. For instance, in the Netherlands, the validity of using trained dogs for certain identification tasks has been called into question. Some factors such as handler influence and environmental conditions can significantly impact the accuracy of a dog's performance, leading to concerns about their reliability in critical situations, so it is considered to be unscientific [130]. Hundreds of volatile, semi-volatile and non-volatile chemical compounds that form the unique human scent are already identified by the scientific community [131] and [132]. Gas chromatography–mass spectrometry (GC/MS) analysis is a testing method that combines gas chromatography and mass spectrometry to identify these substances in a volatile sample, however, it's large heavy equipment and has a high response time which prohibits its use by a UAV. [133] demonstrated a successful differentiation of body odours of two persons with similar lifestyles and activities using an array of E-nose sensors.

Even a small size residue could generate an airborne scent that is detectable when performing a three-dimensional scan by the UAV, a close up ground test might reveal some of the shredded hair or skin cells, those hold microbes and scents foreign to anything found in the environment, human hygienic products would leave similar vapour that can be recognised as a foreign scent. Although the electronic sensors are not as good as the dog nose sensors, it is sufficient to improve the overall performance of the surveillance, and that requires keeping the UAV and its payload sanitised from contamination. The Sniffer 4D Multi-Gas is a system that can detect up to nine gases and particles at once. [134] demonstrated a 16-fold improvement with a commercial explosives detector using a bio-inspired design principle and making the device "sniff" like a dog instead of the conventional steady inspiration for sample intake, to reduce the downwash effect, a vertical tube has been suggested to carry the air sample to the sensor from a few metres distance away from the UAV rotors.

The spatial resolution is dependent on the response time of the sensor and the UAV speed, for a typical sensor with a sample rate of 5 samples per minute the speed of the UAV should be at a very slow speed e.g. 5 metres per minute to achieve a spatial resolution of 1 metre. Placing a vertical tube to pump the air sample into the onboard sensor will further decrease the response time and slow the process. Placing the sensor on the tip of an electrical cable would allow a faster response time by reducing the purge of the tubing volume, the measurement result from the sensor will be transferred to the UAV computer as an electrical signal by the cable as illustrated in Figure 27.

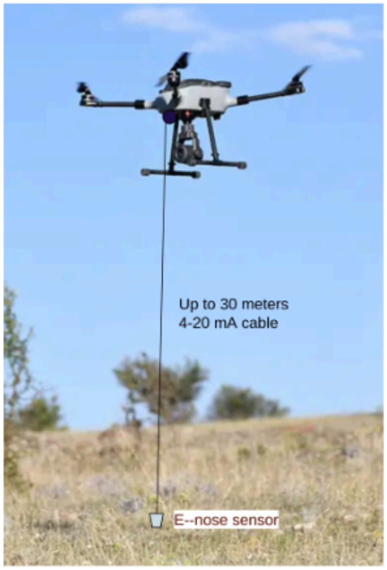


Figure 27. Illustration of vertical air sampling [Author]

C. Machine Model & Image Registration

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.

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.

One example to illustrate sign-cutting by finding an added object using image registration from a video taken at Steveston Harbour, the fishing village on the south arm of the Fraser River in Canada. In the video a truck enters the Harbour wharf and unloads an object on the wharf then the truck leaves the area. If we assume that the surveillance captured an image of the site before the unloading event (Figure 28. A) and returned to its ground base, then on the next day the UAV surveillance performed its routine surveillance and captured an image of the site (Figure 28. B). The automated image registration (Figure 28. C) shows a sign of the unloading event, which will instigate further investigation, and could update the UAV mission to focus on the area looking for more signs.

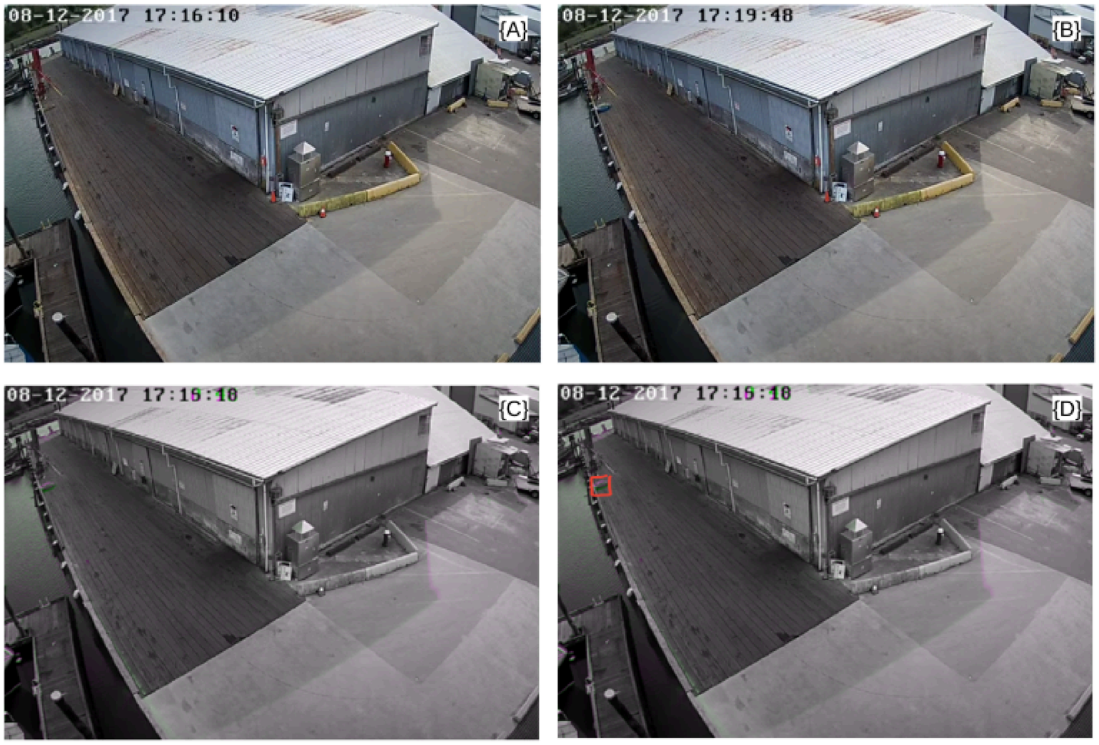


Figure 28. Detecting an object that was added to the scene during the unsurveilled period [114], processed by author

Onboard the UAV machine learning models could instantly identify potential threats, models such as motion and event detection have a high accuracy to provide early warning of suspicious activity. For surveillance UAVs where the perimeter is large, the area will be periodically surveilled, 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.

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. Figure 29. shows a sign of a previous activity detected by a machine model, the original image registered to grayscale, green shows segments with less brightness, and the magenta represents segments with higher brightness [R4].

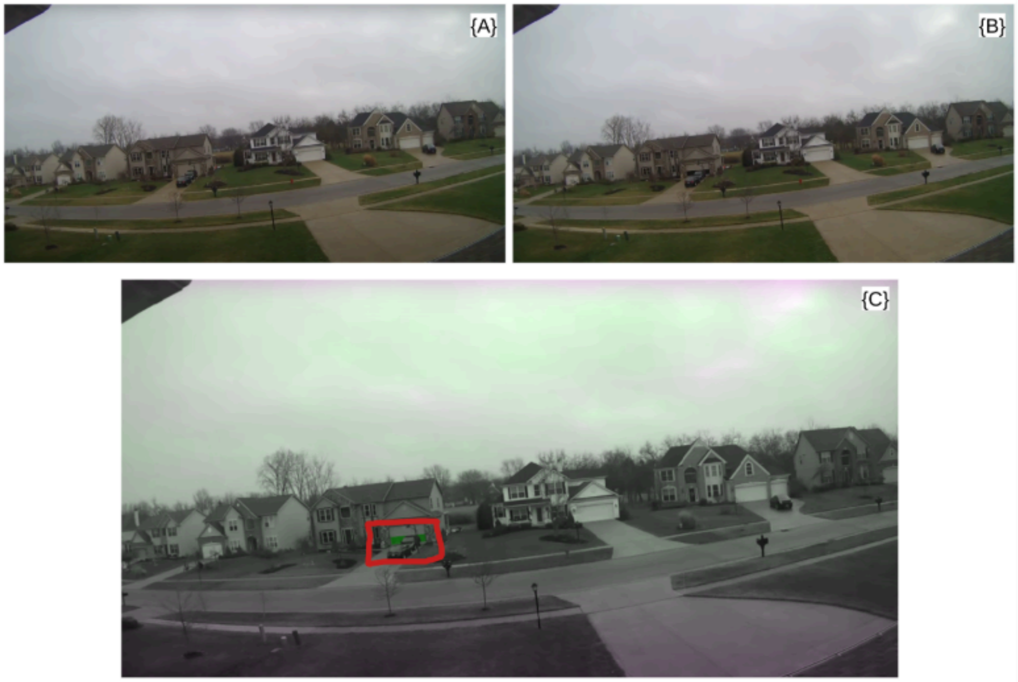


Figure 29. {A} Shows the first surveilled scene, {B} shows the location after time interruption, {C} shows the detected sign [105], processed by author

As the goal is to process a large size of data automatically, intensity-based registration would be the most suitable technique, and detection of the alignment feature points to optimise the geometric transformation has been automated, with a few exceptions, the best-estimated results have been found with the following correlation,

- the less sky, water bodies, or glass in the background, the better detection;
- the less altitude, the less sign size can be detected;
- the more images registered per scene, the better detection.

To quantify the performance of registration the Structural Similarity Index Measure (SSIM) can be used, however, in practical implementation, the number of detecting signs, the size of detected signs, and the recognisability compared to a human expert would be the quality criteria.

4.5. Discussion

The proposed approach has the potential to increase the efficiency of borders and energy pipeline surveillance, currently, the surveillance videos are not fully reviewed, and the computerised video analysis process is focused on detecting objects (humans, cars). Integrating signs detection would have a positive impact with minimal added cost. The tolerance of the system is easily controllable, depending on the alert status and the availability of verification manpower, the amount of false positives detected could be adjusted [R4].

The most important part of such a system is training the CNN, based on previous visual recognition projects a variety and large number of image datasets is required for the training (5,000-10,000 images), preferably the training images to be taken by the same surveillance UAV to keep as much similarity as possible to the terrain characteristics and flight altitude, therefore increase the overall accuracy of signs identification, the dataset images should include images with made up signs simulating the expected signs to be identified by the CNN, and images with no signs at all. The system is expected to yield good results immediately upon implementation and is designed to be updatable. The original training dataset can be regularly refreshed by incorporating new images from real-world experiences, including instances of both false positive and false negative identifications. This ensures that whenever the system incorrectly identifies a sign or fails to recognise one, it can learn from these mistakes. Those images should be added to the original training dataset and re-train the CNN so the same identification mistakes will not get repeated, this way the system will be in continuous learning, and with more time it will compound experience and increase accuracy.

The main challenge for UAV surveillance is weather conditions which could affect the flight itself or block the camera view, synthetic aperture radar (SAR) penetrates through the clouds and foggy weather, some other challenges like the four seasons, and the sign's size, shape, angle, age, and signs caused by border agents themselves, and many other factors might cause false identifications but as the training dataset increase by adding those new false identification images to it, the errors will decrease [R4].

The smugglers are forensically aware, as with any other deterrent technology the smugglers will try to minimise its effect. In this case using a sort of camouflage to hide the signs is expected, a possible method is holding a tree branch while walking to erase and camouflage their footprints or attach objects to the rear of their cars in order to disturb the tire impression as shown in Figure 30.

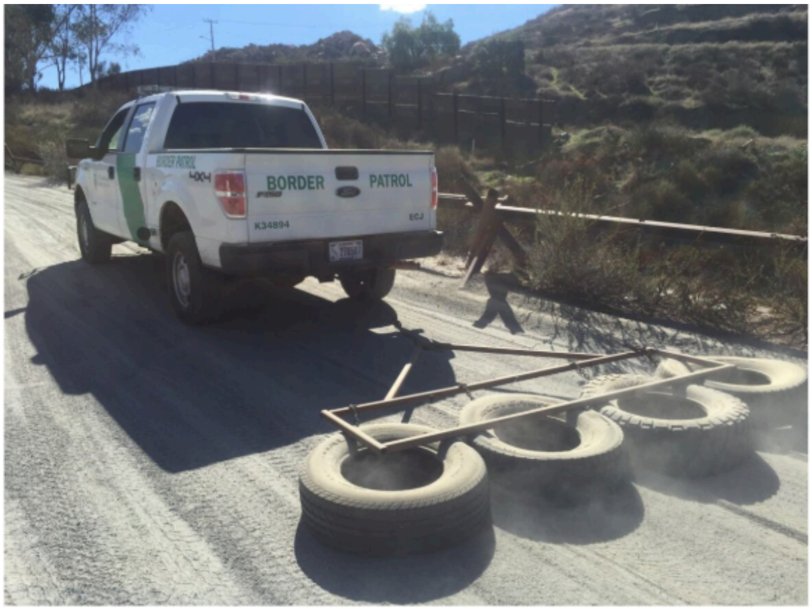


Figure 30. Refreshing the road soil so footprints show up more easily [135]

There is a possibility to train the CNN to identify such a camouflage as the soil is freshly disturbed so it’s still distinctive from the environment. A similar concept could be applied to other specialized cameras, such as spectral cameras, which capture hundreds of different light wavelengths for the same scene. This capability allows convolutional neural networks (CNNs) to detect specific chemical compositions, enabling the identification of many signs using hyperspectral images. Many indicators that might be missed by other technologies can be detected, making camouflaging extremely challenging.

Signs such as soil scrapes, bruised grass, broken twigs, small rocks displaced, wet ground, and clothing fibers are all detectable disturbances. For example, detecting disturbed soil in a different color wavelength from the surrounding area has been demonstrated, although no accuracy metrics for true detection have been established. Additionally, objects with differing textures are much easier to detect using spectral technology. Hyperspectral cameras produce image arrays that are significantly larger than standard camera videos, highlighting the urgent need to automate the sign-cutting process.

The automated intensity-based image registration could improve the sign-cutting process through UAV surveillance imagery, feature/point-based registration could produce a higher SSIM score but has consistently shown less overall detectability, the natural changes in sun light would create residual misalignment usually with lower SSIM score which could allow an identifiable distinguishing threshold score that allows the system to discard certain misregistration changes. The main advantages are the affordable computational power for large image data, the ability to automate, and the sign detectability. The disadvantage is the signal-to-noise ratio, which results in high false positives.

Chemical sensing UAVs are still an emerging technology especially when implemented for unidentified scent tracking, nonetheless, it could produce some sign clues if it's targeted specific chemicals e.g., explosive trinitrotoluene (TNT), narcotics, or hydrocarbons. The main disadvantage is the high cost, precision, and slow response time. The speed of chemical scanning could be improved by using multiple sensors in an array, but this is limited to niche applications and limited surveillance area coverage.

4.6. Conclusion

We can summarise the benefits of the suggested concept mainly by its effectiveness and speed, and the ability to process large amounts of video footage that is very difficult to process otherwise by manual methods. The main limitations are weather conditions, and discarding signs made by other natural sources (e.g. wild animals).

1. Automated image registration can detect signs from surveillance imagery. and can process big data of periodic surveillance videos with minimal human supervision.

2. The overall accuracy is not measured yet, but we suggest that an approach similar to the Large Scale Visual Recognition Challenge (LSVRC) could be used to measure the accuracy and to evaluate algorithms for sign detection.

3. Chemical sensing technology might be useful in certain situations, but it's not mature enough, and is far from practical for detecting and tracking scents of border intrusions.

Comparing the life cycle costs of UAVs with manned aerial systems reveals inherent advantages due to the absence of life support systems, resulting in reduced equipment, weight, size, and overall expenses. However, concerns arise regarding accidents and crash rates, often attributed to ground pilot errors or mechanical failures. Over the past three decades, strides in safety standards and pilot training have mitigated these risks for UAVs. From a cost perspective, despite recording 23 crashes per million flying hours, the RQ-4 Global Hawk UAV maintains a competitive edge per flying hour compared to the P-8 manned navy aircraft.

The investigated technologies in this chapter are promising, given the industry rate of evolving, autonomous sign-cutting and tracking by surveillance UAVs might be possible in the foreseeable future. However, despite being important the topic remains understudied and the author finds the results supporting **Hypothesis 1** 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". and support **Hypothesis 3** which posits that "Machine vision can be applied for clues detection, to aid automating the process of sign-cutting in a perimeter surveillance imagery data", and identify some of the current limitations to achieving autonomous sign-cutting challenging **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".

5. CASE STUDY OF A PROPOSED SOLUTION: EXAMPLE OF JORDAN

Jordanian border security is a historic continuous challenge, as the threats rapidly increase both in number and sophistication; advanced modern technologies could help to obtain an adequate level of protection. Securing the outdoor perimeter of any facility, especially if it is with large dimensions. Today, there are many sites with large areas that fall into this long perimeter range and require a high level of security (e.g. critical infrastructure, residential areas, international borders, rivers, etc.). Designing a comprehensive solution based on the Unmanned Aerial Vehicle (UAV) system has the potential to help solve many of the problems associated with current conventional security systems in terms of efficiency, reliability, and cost. The proposed plan is to study the concept of the UAV systems applied in different environmental conditions to improve the efficiency of the UAV systems. The proposed UAV system is based on modern methods and principles to reach the basic goal of surveillance covering the Jordanian border. In this chapter, we have applied integer programming optimisation techniques to support the overall project design in minimising the number of bases and optimising the number of selected surveillance technologies. The transition from manned vehicles to UAVs for surveillance purposes has been more widely adopted by the US military than other potential operations, as shown in Figure 31 below.

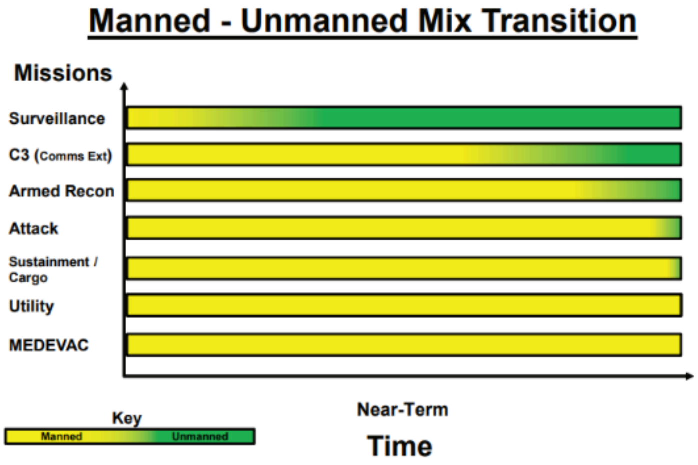


Figure 31. US Army transition from manned to unmanned aerial vehicles [136]

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. Figure 32. shows the topography of Jordan [R2].

To cover the whole length, 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 perimeter, as well as multiple layers of technology including cameras and other types of sensors both permanent fixed and mobile sensors carried on ground and aerial vehicles. The proposal is to optimise the number of UAVs that are needed for surveillance while at the same time optimising the number of UAVs operational and maintenance bases together with the quality and quantity of technologies carried by each vehicle. The approach is evaluated from an engineering technological analysis accompanied by an economic constraint. For the complexity of the system, we will use a heuristic method whenever a certain estimated or exact information is not available, while a good practical estimation can be made.

The large variety of sensors and the frequent circumstances changes require multiple optimisation needs for the decision maker, therefore creating a model to prioritise different options will be helpful, the suggested model is capable of optimising a large set of variabilities. For each scenario, the decision maker would need to input the distance between the number of potential areas for ground bases and the range of the UAV in kilometres and the model will generate the minimum number of ground bases that will cover the whole segment. For model B, the decision maker has to enter the operational value for each technology and its cost, as well as the budget, and the model will select the sensors with the maximum overall value for the given budget.

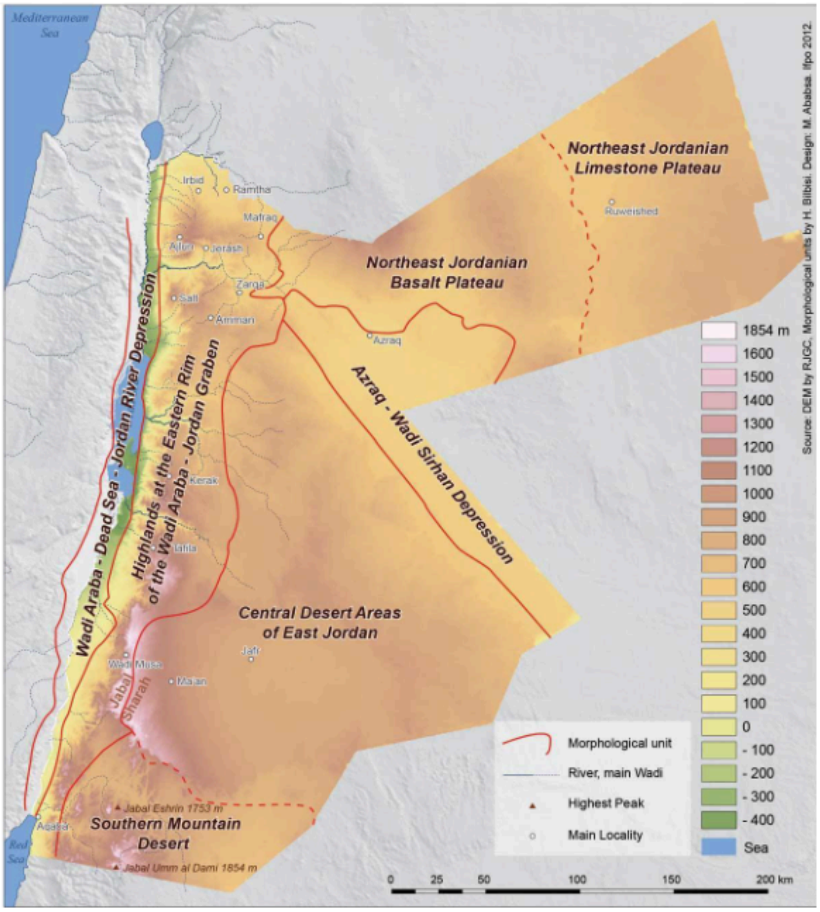


Figure 32. Topography of Jordan [137]

5.1. Technologies Selection

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.

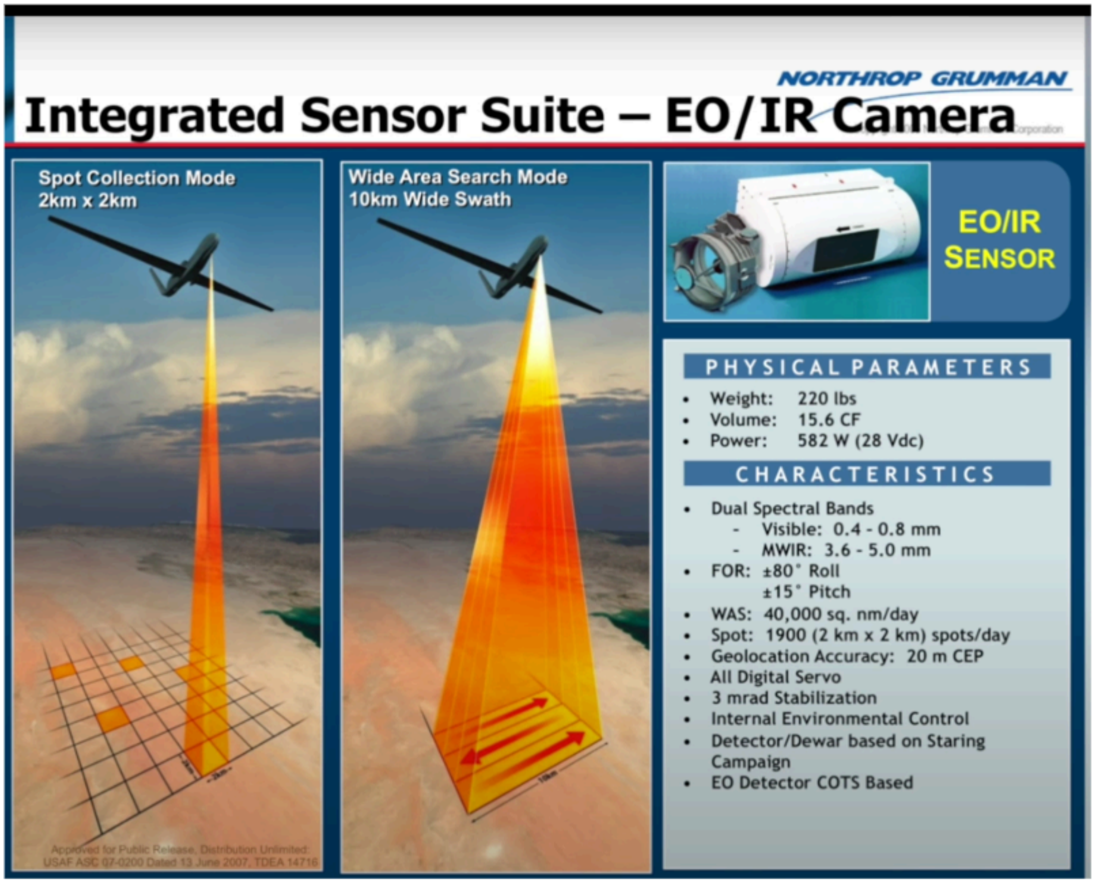
The evaluation sequence is as follows,

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.

When a segment of the border is to be evaluated consideration of the terrain of both sides of the borders, in the case of Jordan, the majority of its border is a flat desert plateau and has no natural features that separate both sides, for such segment a camera with night vision would be sufficient and add great value while for a heavy forest segment a LIDAR technology would add the most value [R2].

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. For many technologically advanced countries, security cameras are a better option than using costly and deadly mines. It can also reduce the need for additional physical obstacles or fences, it's difficult for intruders to avoid being caught by a UAV camera. Advances in machine learning for recognition and video analytics software has reduced the number of human analysts needed to maintain a sufficient level of security. Electro-optical/infrared (EO/IR) systems are imaging technologies that combine electronics and optics to detect, identify, and track targets in the visible light and infrared spectrum. Figure 33. shows the characteristics of electro-optical/infrared sensors used for aerial imaging.


NORTHROP GRUMMAN
2km
2km
10km

Integrated Sensor Suite – EO/IR Camera

Spot Collection Mode
2km x 2km

Wide Area Search Mode
10km Wide Swath

EO/IR SENSOR

PHYSICAL PARAMETERS

- Weight: 220 lbs
- Volume: 15.6 CF
- Power: 582 W (28 Vdc)

CHARACTERISTICS

- Dual Spectral Bands
  - Visible: 0.4 - 0.8 mm
  - MWIR: 3.6 - 5.0 mm
- FOR: ±80° Roll
  ±15° Pitch
- WAS: 40,000 sq. nm/day
- Spot: 1900 (2 km x 2 km) spots/day
- Geolocation Accuracy: 20 m CEP
- All Digital Servo
- 3 mrad Stabilization
- Internal Environmental Control
- Detector/Dewar based on Staring Campaign
- EO Detector COTS Based

Approved for Public Release, Distribution Unlimited:
USAF ASC 07-0200 Dated 13 June 2007, TDEA 14716

Figure 33. Electro-optical/infrared camera used for aerial imaging [138]

The basic job of a camera is to create an image from the light, in order to capture the most amount of light, a monochrome “black & white” complementary metal–oxide–semiconductor CMOS sensor (or other technologies such as charge coupled device CCD) is used. To create coloured images 25% red, 50% green, and 25% blue filters (a Bayer filter array) are placed over the monochrome sensor, blocking about two-thirds of the light intensity. For the same sensor size a trade-off between light sensitivity and coloured information must be made, for a well-lit area, colour information (spectral information) is usually more important to optimise than light intensity.

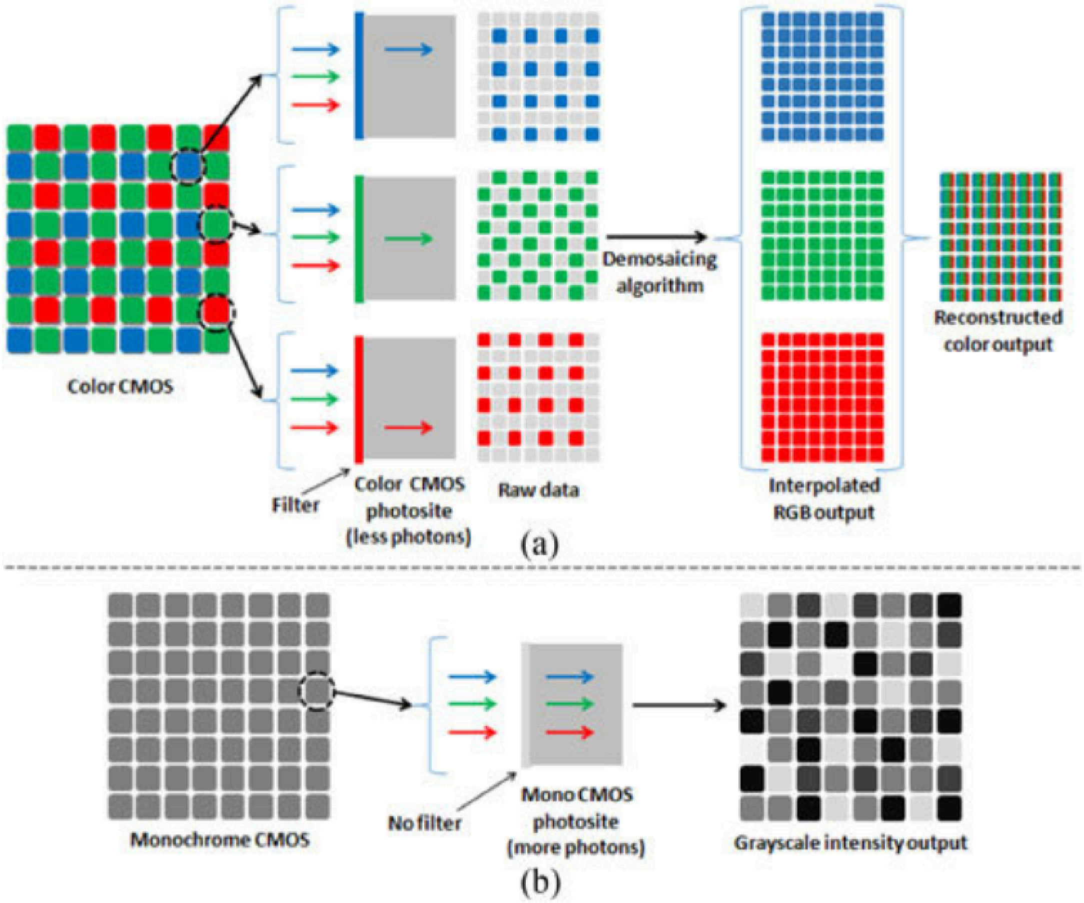

Color CMOS
Filter
Color CMOS photosite (less photons)
Raw data
Demosaicing algorithm
Interpolated RGB output
Reconstructed color output
(a)
Monochrome CMOS
No filter
Mono CMOS photosite (more photons)
Grayscale intensity output
(b)

Figure 34. Principle of (a) colour and (b) monochrome CMOS camera [139]

Practically most sensors are sensitive to the visible part of the electromagnetic spectrum and to a lesser extent to the near infrared and near ultraviolet. Figure 35. shows the wide range of UV and IR wavelengths detectable by sensors, many sensors are specifically designed to detect specific wavelengths beyond the visible. Ultraviolet, short, medium, and long infrared wavelengths can also be captured which is particularly useful for capturing thermal images at infrared wavelengths. One of the most important aspects of the camera sensor is the resolution (pixel size) as the detection of an object depends on this, ideally smaller pixel size and higher pixel density (pixel per inch - PPI), and larger sensors help to identify smaller objects on the ground for the same focal length and flying height above the object.

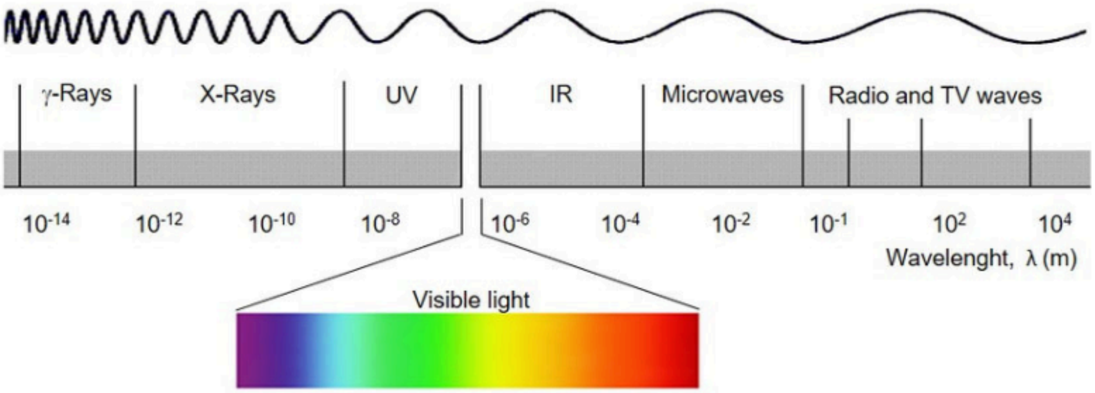


Figure 35. A wide portion of UV and IR wavelengths are detectable by sensors [140]

To overcome the limitations of the photosensitive sensor a different type of lens is usually used to focus the light onto the sensor, focal length, aperture and depth of field are important considerations when selecting the lens. In addition to object size, object detection depends on two camera specifications and one flight specification,

- Pixel size: the distance between two pixels centres in (m);
- Focal length: the distance between the lens and the sensor when the object is in focus in (m);
- Flight height: the distance between the camera and the the object in (m);

Ground Sensing Distance GSD = (Pixel size x Flight height / Focal length).

As a practical rule of thumb, in a well-lit area, successful object detection happens when the object width is at least 3 times larger than the GSD. This is the best-case scenario, in practice, many other factors can disturb the image, such as the weather conditions, data transmission and handling, and camouflage. Having multiple overlapping images from different angles could help overcome disturbances and result in successful object detection.

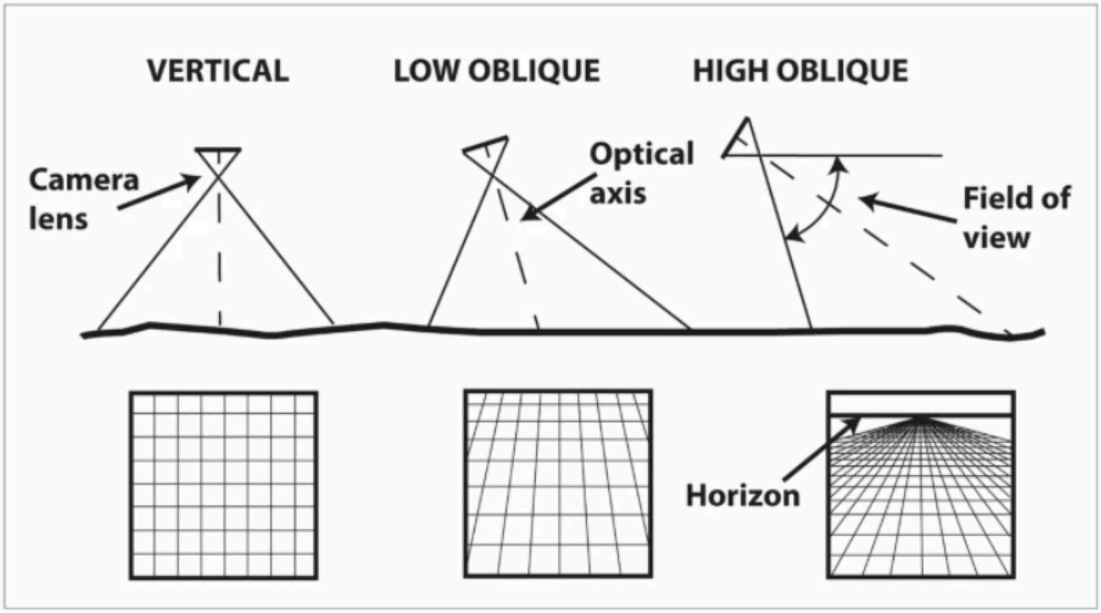


Figure 36. The appearance of grid lines from different lens orientations [141]

The real value of an image comes from its interpretation, and orientation Figure 36. and it's important to collect other types of data (metadata) for each image, the time, location, focal length (focal length is commonly controlled and frequently adjusted), audio and other relevant data. The Global Positioning System (GPS) has made collecting precise location for image acquisition possible adding great value to aerial imaging. In flat terrain it is easier to estimate the height of the camera above the object and its orientation, but in many cases, the terrain is variable in height and orientation requiring special equipment and/or techniques to estimate an accurate enough object size, and what is the desired accuracy and precision of object delineation. The altitude above the object would affect the scale in the image. Figure 37. shows how different terrain affects the distance between the lens and the object [R2].

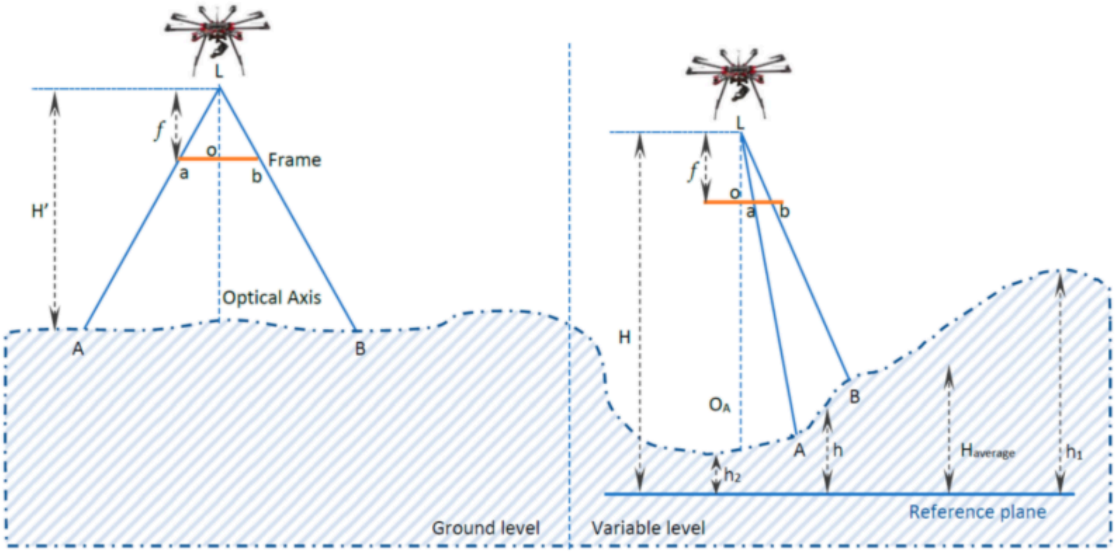
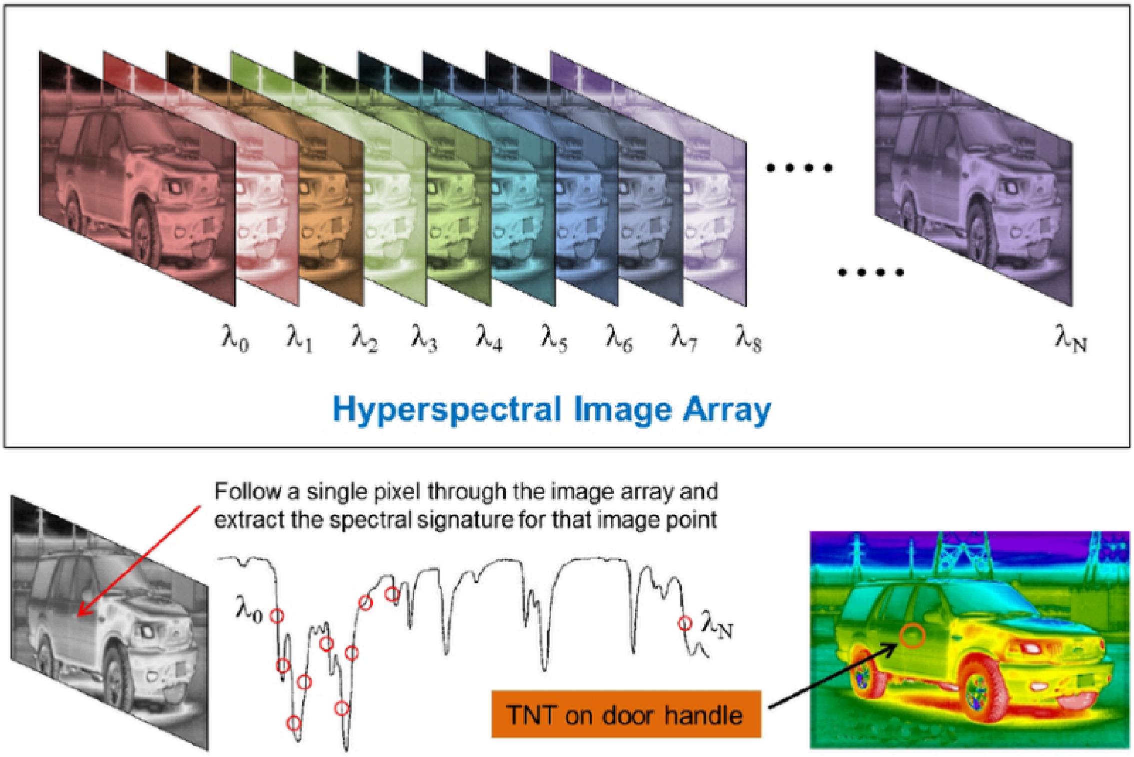


Figure 37. Difference between (Left) flat terrain imaging and (Right) variable terrain imaging [142]

More spectral information increases the chances of object detection, when many spectral (Hyperspectral) wavelengths are used to create an image, a signature of the chemical composition can be identified as each chemical element or molecule has its unique reflection of specific wavelengths and absorption of other wavelengths, such images help to detect specific chemicals (e.g. explosive material) and camouflaged items, by comparing the received spectral with a known spectral signature. Figure 38. shows how a TNT explosive residue could be detected by analysing a hyperspectral image array.



λ_0 λ_1 λ_2 λ_3 λ_4 λ_5 λ_6 λ_7 λ_8 λ_N
Hyperspectral Image Array
Follow a single pixel through the image array and extract the spectral signature for that image point
λ_0
λ_N
TNT on door handle

Figure 38. Detecting chemical signatures in Hyperspectral image array [143]

In terms of detecting signs and clues such as soil disturbance, spectral image arrays could provide additional data when the conventional image processing fails to register the phase difference or intensity, image registration at each wavelength also improves the confidence of the detected change, especially by avoiding shadows in the scene. In [144] the level of discriminative information that could be extracted from the object texture using spectral imaging was investigated. Figure 39. shows disturbed soil in visual imaging compared to spectral images.

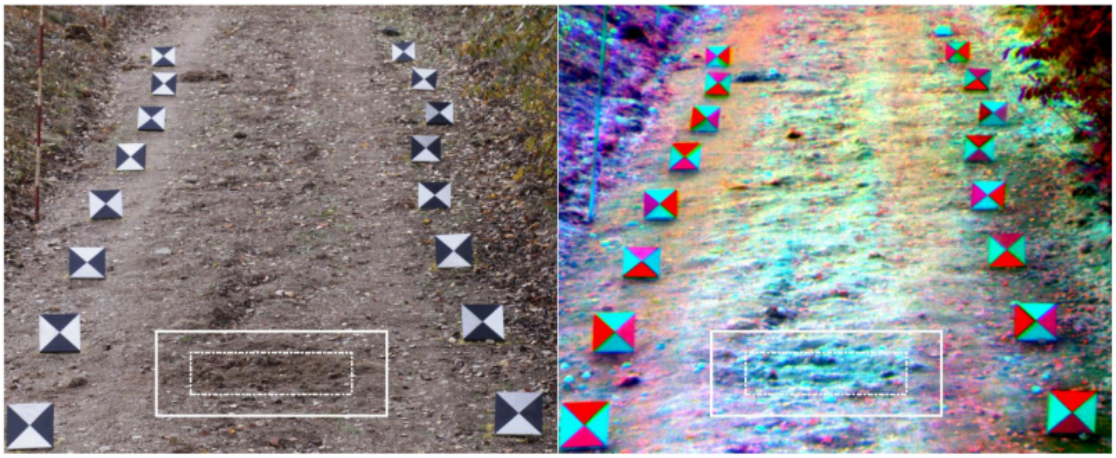


Figure 39. Visual image (left) spectral image (right) of a newly disturbed soil [144]

A significant part of each year the weather conditions do not allow clear imaging within the visible range (especially from high-altitude flights), SAR is a type of radar technology that can create images even through media (fog, clouds, tree canopies, storms…etc), as it uses much lower frequencies of the electromagnetic spectrum (micro and radio waves) that can penetrate most of the low visibility weather conditions (not useful for objects under the surface of water bodies). Unlike visible light which is mostly supplied by the sun's illumination, SAR sends its waves and receives their reflection back to create an image that reconstructs the shape of the object, this advantage allows imaging during the night (all-weather, day-and-night imaging sensors) however SAR images are monochrome and has a poorer resolution (around 1 foot resolution) making it difficult to detect signs at this resolution but allowing the detection of large objects or people, Figure 40. is a SAR image showing four people detected.

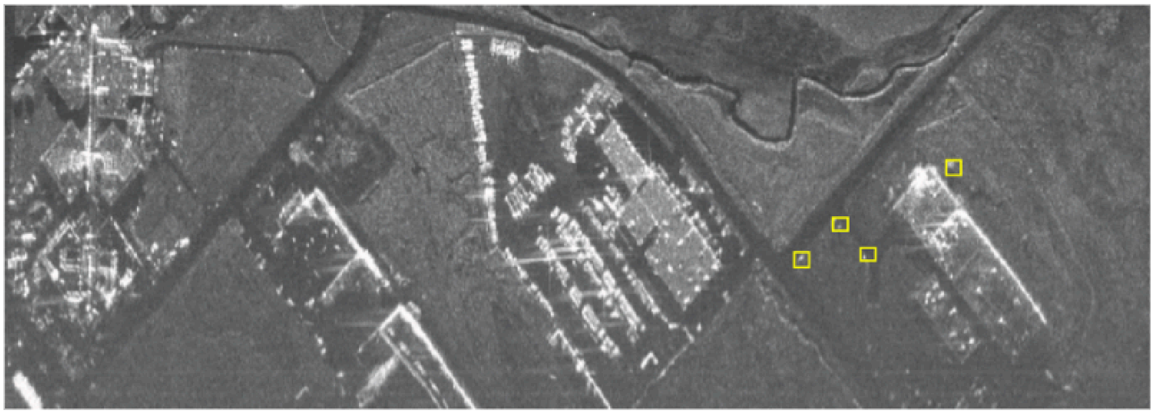
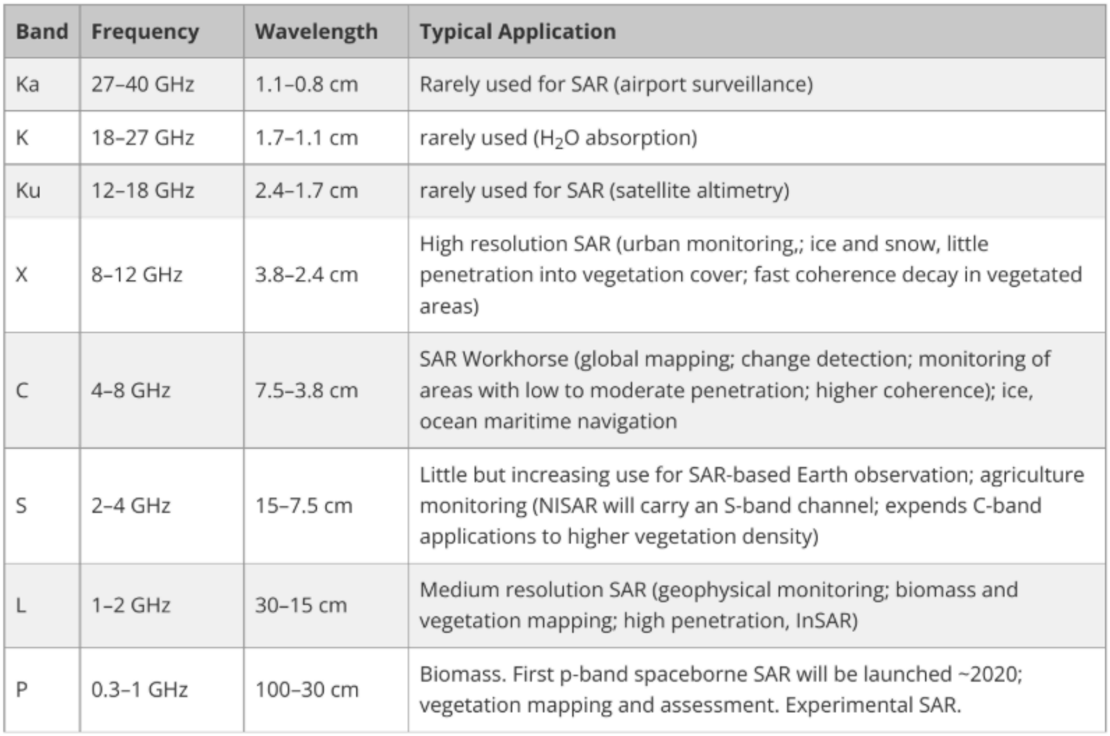


Figure 40. SAR image showing four people detected. [145]

Depending on the specific application, certain electromagnetic wavelengths could be selected to optimise the performance beyond the general advantages of SAR technology, the European Remote Sensing SAR is a satellite with a ground range resolution of about 25 m and a maximum azimuth resolution of 5 m, while NASA's uninhabited aerial vehicle (UAVSAR) has a range resolution of about 2 m, a range bandwidth of 80 MHz, and a range swath of over 16 km. The radar is fully polarimetric and has a centre frequency of 1.2575 GHz, Table 4. shows the typical application of SAR at different wavelengths.

Detecting vehicles prints and oil spills from a pipeline are typically successfully performed tasks by the radar, however, the potential future resolution would allow detected smaller signs, it's worth mentioning that the Gartner Group report in 2023, most of the earth observation technologies are still at the innovation trigger stage, SAR is on the peak of inflated expectations, that and the high cost might limit its use to areas where the flight altitude required to be above cloud level and other special niches. The all-weather low visibility capability will maintain demand for this technology despite the cost.



Band	Frequency	Wavelength	Typical Application
Ka	27–40 GHz	1.1–0.8 cm	Rarely used for SAR (airport surveillance)
K	18–27 GHz	1.7–1.1 cm	rarely used (H_2O absorption)
Ku	12–18 GHz	2.4–1.7 cm	rarely used for SAR (satellite altimetry)
X	8–12 GHz	3.8–2.4 cm	High resolution SAR (urban monitoring,; ice and snow, little penetration into vegetation cover; fast coherence decay in vegetated areas)
C	4–8 GHz	7.5–3.8 cm	SAR Workhorse (global mapping; change detection; monitoring of areas with low to moderate penetration; higher coherence); ice, ocean maritime navigation
S	2–4 GHz	15–7.5 cm	Little but increasing use for SAR-based Earth observation; agriculture monitoring (NISAR will carry an S-band channel; expends C-band applications to higher vegetation density)
L	1–2 GHz	30–15 cm	Medium resolution SAR (geophysical monitoring; biomass and vegetation mapping; high penetration, InSAR)
P	0.3–1 GHz	100–30 cm	Biomass. First p-band spaceborne SAR will be launched ~2020; vegetation mapping and assessment. Experimental SAR.

Table 4. Shows the typical application of SAR at different wavelengths [146]

Physical bodies with a temperature above absolute zero emit thermal radiation. People, animals, vehicles, and electronic devices are all sources of thermal radiation. The power of this radiation depends on the body's emissivity (its ability to emit energy), surface area and temperature, as shown in the following equation,

$$P = \sigma * \varepsilon * A * T^4$$

P: is the power of the body's thermal radiation.

σ: is the Stefan Boltzmann constant, equal to $5.670367 * 10^{-8}$.

ε: is the emissivity of the substance.

A: is the surface area of the body.

T: is the temperature of the body (Kelvins).

Thermal radiation is emitted over a relatively wide range of wavelengths and the intensity of the radiation is best captured at certain wavelengths, while human body peak thermal radiation is in the long wave infrared (LWIR), jet engine exhaust radiates in the medium wave infrared (MWIR), and the sun peak radiation is on the visible wavelengths. Each segment of these wavelengths behave differently, and the fact that glass is not transparent to thermal radiation dictates the design and material of the focal lenses and the reflected rays in the image.

Gartner's Hype Cycle is a framework that illustrates the evolution of a technology through various stages, from its inception to eventual decline. It begins with the Innovation Trigger, where a breakthrough or development sparks initial interest and excitement. This is followed by the Peak of Inflated Expectations, where expectations soar as early adopters experiment with the technology, often leading to exaggerated claims about its potential. However, this is soon followed by the Trough of Disillusionment, where the limitations and challenges of the technology become apparent, resulting in a decrease in interest and investment. As organisations gain a more realistic understanding of the technology's capabilities and limitations, it progresses to the Slope of Enlightenment, where practical applications begin to emerge and more stakeholders recognise its value. Finally, the cycle culminates in the Plateau of Productivity, where the technology reaches maturity and achieves widespread adoption, but it may also face decline and obsolescence as newer innovations emerge. This cyclical pattern serves as a valuable guide for businesses and investors, helping them navigate the often unpredictable landscape of technological advancement and making informed decisions based on the current stage of a given technology. The tool helps to track the maturity and potential of certain technologies. Figure 41. shows the development of commercial UAVs 2017-2022.

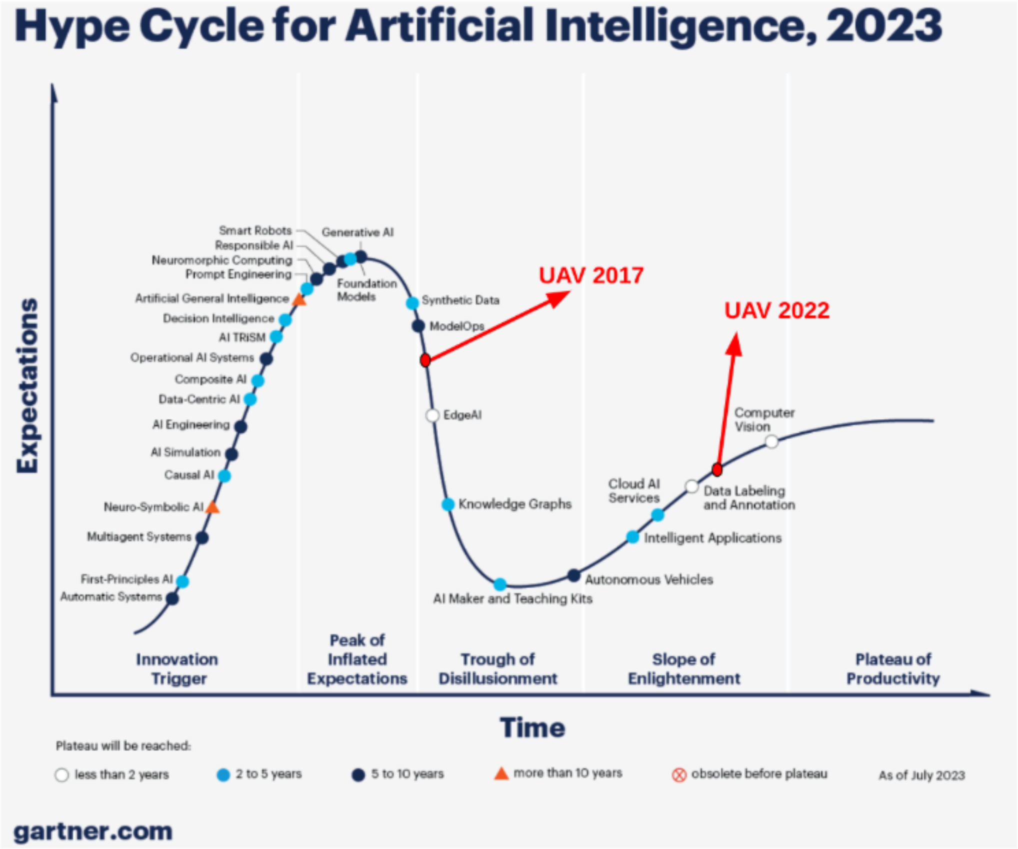
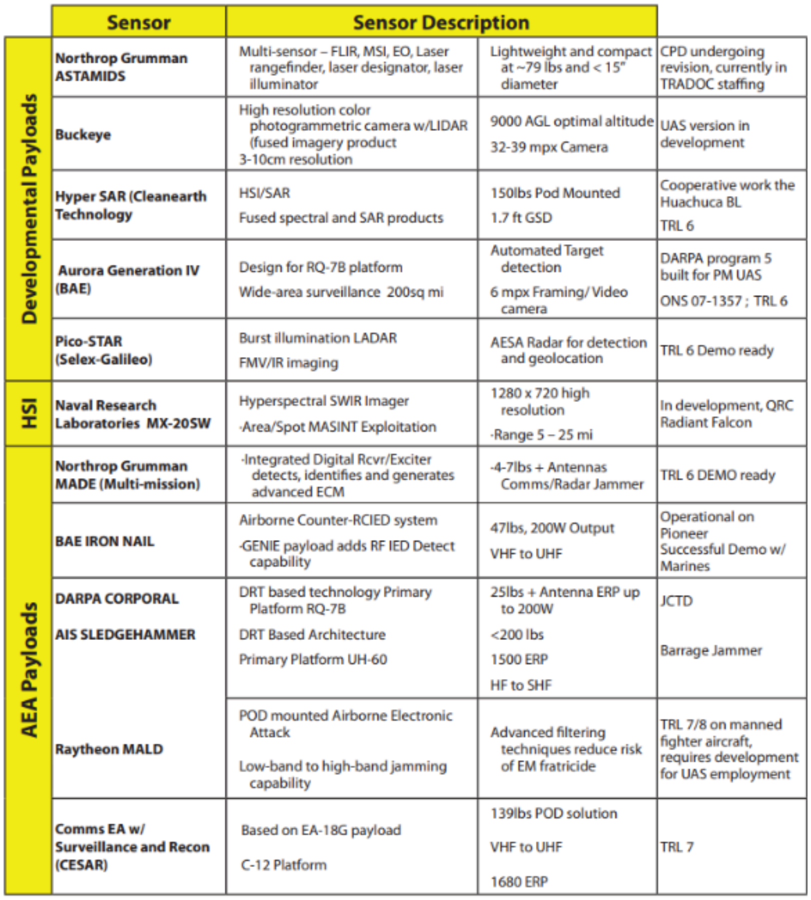


Figure 41. The development of commercial UAVs 2017-2022 Gartner Group, processed by [Author]

The Gartner hype cycle could also give an insight into the future potential of a technology aiding the designers to design with the consideration of future upgrades, border agencies have been using roadmaps to optimise the implementation of current systems with a futuristic vision of potential upgrades, listing mature and expected technologies.Surveillance applications increasingly rely on Unmanned Aerial Vehicle (UAV) technology, which serves as the foundational tool for this model. UAVs exhibit a diverse range of shapes and configurations, with flight ranges varying from a few metres to several tens of thousands of kilometres. Correspondingly, their payload capacities also vary significantly, allowing for the integration of a wide array of technologies and sensors.

To optimise field results, a flexible and effective model can be implemented as a pilot project for experimental purposes. This model is designed to be scalable, accommodating various operational requirements and magnitudes. So the model can start with one UAV carrying one camera and using one ground base for operation and maintenance to a multiple of each and additional equipment and technologies depending on the budget and risk level.

Consideration should be given to incorporating a broader range of technologies based on potential developments, particularly those that are underdeveloped but may prove valuable to our model. An illustrative example is the “Ground-Effect Vehicle,” which is well-suited for UAV applications. While the phenomenon of ground effect has been known for decades, it has not yet been fully exploited, especially in UAV design. This approach could mitigate one of the primary concerns of manned Ground-Effect Vehicles, the risk of hazardous accidents involving human pilots operating at low altitudes. In my point of view, this technology would have a potential improvement in the field of perimeter security using UAVs, and such could be added to the model at a later stage. The following Table 5. shows some specific sensor payload characteristics, the sensor rating for the selection model depends highly on the application details and the interoperability of the whole system sensors combined, the system should be responsive to the current and expected operational demand [R2].



	Sensor	Sensor Description		
Developmental Payloads	Northrop Grumman ASTAMIDS	Multi-sensor – FLIR, MSI, EO, Laser rangefinder, laser designator, laser illuminator	Lightweight and compact at ~79 lbs and < 15" diameter	CPD undergoing revision, currently in TRADOC staffing
	Buckeye	High resolution color photogrammetric camera w/LIDAR (fused imagery product 3-10cm resolution	9000 AGL optimal altitude 32-39 mpx Camera	UAS version in development
	Hyper SAR (Cleanearth Technology	HSI/SAR Fused spectral and SAR products	150lbs Pod Mounted 1.7 ft GSD	Cooperative work the Huachuca BL TRL 6
	Aurora Generation IV (BAE)	Design for RQ-7B platform Wide-area surveillance 200sq mi	Automated Target detection 6 mpx Framing/ Video camera	DARPA program 5 built for PM UAS ONS 07-1357 ; TRL 6
	Pico-STAR (Selex-Galileo)	Burst illumination LADAR FMV/IR imaging	AESA Radar for detection and geolocation	TRL 6 Demo ready
HSI	Naval Research Laboratories MX-20SW	Hyperspectral SWIR Imager ·Area/Spot MASINT Exploitation	1280 x 720 high resolution ·Range 5 – 25 mi	In development, QRC Radiant Falcon
AEA Payloads	Northrop Grumman MADE (Multi-mission)	·Integrated Digital Rcvr/Exciter detects, identifies and generates advanced ECM	-4-7lbs + Antennas Comms/Radar Jammer	TRL 6 DEMO ready
	BAE IRON NAIL	Airborne Counter-RCIED system ·GENIE payload adds RF IED Detect capability	47lbs, 200W Output VHF to UHF	Operational on Pioneer Successful Demo w/ Marines
	DARPA CORPORAL AIS SLEDGEHAMMER	DRT based technology Primary Platform RQ-7B DRT Based Architecture Primary Platform UH-60	25lbs + Antenna ERP up to 200W <200 lbs 1500 ERP HF to SHF	JCTD Barrage Jammer
	Raytheon MALD	POD mounted Airborne Electronic Attack Low-band to high-band jamming capability	Advanced filtering techniques reduce risk of EM fratricide	TRL 7/8 on manned fighter aircraft, requires development for UAS employment
	Comms EA w/ Surveillance and Recon (CESAR)	Based on EA-18G payload C-12 Platform	139lbs POD solution VHF to UHF 1680 ERP	TRL 7

Table 5. Sensors payload characteristics [147]

5.2. The Design Aspects

To select the optimal surveillance UAVs for the border we need to identify the following,

Demarcation of the border line, identification of potential threats, sensor capabilities to detect potential threats, methods of deterrence, methods of delaying threat sources, methods of defeating the threats, methods of mitigating the effects of an attack, negative feedback markers, potential future upgrades and integration, and the levels of security for the information.

Demarcation of the borderline. Full dimensions must be identified for the border, the threats from aerial - and space - as well as from underground incumbent a demarcation of border lines in these domains, practically the border lines imply a specified operational space around them. In an extreme case, the optimal way to detect a missile is at the moment of launching it thousands of kilometres away. One approach is to divide the UAV operation area horizontally based on the levels of required surveillance, and vertically into ground, underground, and airspace levels, so the integration of the UAV into the other layers of the system (physical fences, intelligence, ground devices, etc.) will be optimised.

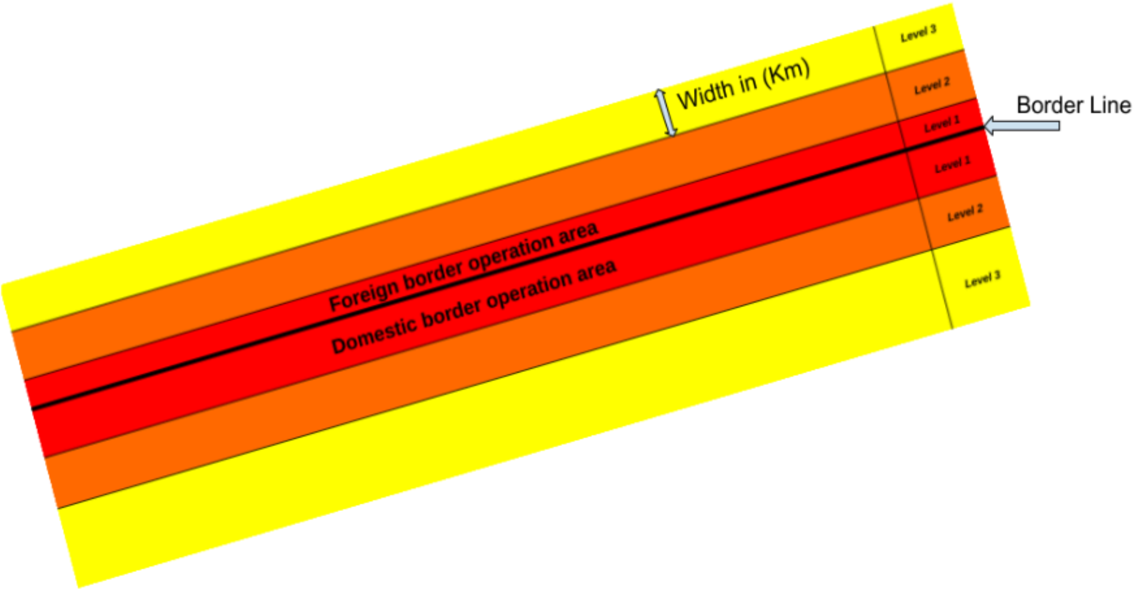


Figure 42. Illustration of the UAV operational ground area around the borderline [Author]

To identify the potential threats. A list of potential threats with the level of risk for each would be identified by analysing the history of incidents at the said border and also analysing the incidents at similar borders around the world, this will ultimately predetermine the selection of security technologies and justify the spending. The UAV would look for threats of intrusions on a foreign ground or aerial vehicles, people, animals, objects (carried by animals or wind), fire, hazardous materials, or radiation. also any suspicious traces, activities, and markings such as foreign objects, digged holes, broken plants, disturbed soil, and foot impressions.

Identify the ability of sensors to detect potential threats. A variety of sensors can contribute to the detection of a threat, an overall assessment of the probability of contribution to each of the listed threats multiplied by their level of risk.

$$\text{Value of the sensor} = \sum (\text{contribution to detect } T_n) \times (\text{probability of } T_n) \times (\text{risk level of } T_n)$$

It is very important to keep in the design the concept of "hide and seek" as many threats are initiated by cunning consciences who gather intelligence and try to achieve their goals by least expected methods.

Identify methods of deterrence. Deterrence is the main priority of the system, it is achieved by assuring an appropriate punishment for any criminal intruder and instilling fear of the worst outcome as a consequence of their intrusion. To evaluate the effectiveness of a deterrent technology an estimate is made of the level it is likely to induce in potential intruders, multiplied by the number of potential intruders who would be affected.

$$\text{Effectiveness} = \text{Deterrence level} \times \text{number of affected intruders}$$

Identify methods to delay threat sources. The surveillance UAV is often the first contact with the threat source and it has the potential to perform some immediate response, therefore equipping the UAV with interaction technologies to communicate certain messages to the intruders and delay their advances toward the secured perimeter.

Identify methods of defeating the threats. Many of the modern time threats are swift, not allowing for conventional response, it should be treated with disabling countermeasures seconds after its detection to fully block and defeat it.

Identify methods to mitigate the effects of an attack. Minimising the effect of an attack should be considered by including UAV technologies that expedite recovery (e.g. first aid, fire extinguishing… etc). An accurate risk assessment is necessary to budget the ratio of cure measures to prevention measures.

Identify negative feedback markers. For the system to be adaptable, a unified measurable marker should be identified to evaluate the performance of each input; this feedback loop could help improve the system and reduce inefficiencies.

Identify potential future enhancements and integrations. As many technologies double their capabilities every few years, the discounted value of future capabilities should be calculated and compared with the selected current technologies on a cost-to-benefits ratio merits.

Identify levels of information security. For security, the system capability is not sufficient for optimal results, the secrecy element is very important as the system deals with human psychology, a primitive technology may outperform an advanced one if unexpected by intruders. Depending on the goals some technologies deter intruders best when publicised, while other technologies deter best by yielding their performance in secret. To estimate the total financial cost and payback of the project, it would be necessary to estimate the following inputs,

1. Total initial cost
2. Yearly operation & maintenance costs
3. Lifespan of the project
4. Yearly revenues (cost of the prevented crimes)
5. Salvage value (at the end of lifespan)
6. Interest rate

5.2.1. ILP Model A

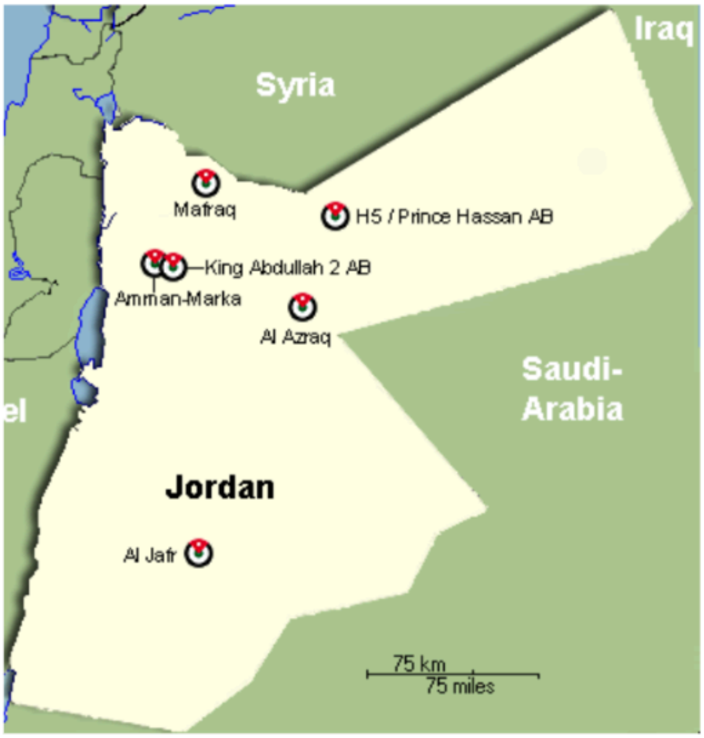


Figure 43. Map of the Royal Jordanian Air Force bases distribution [148]

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].

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:

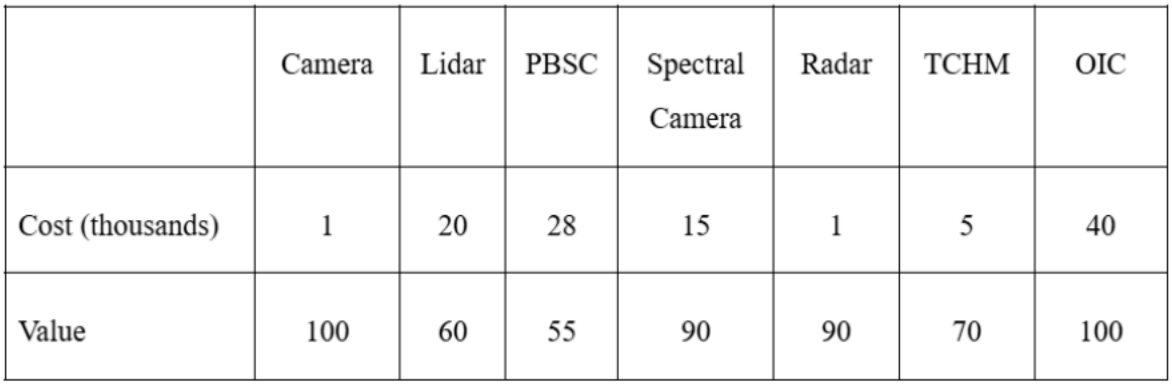
$$Minimise \sum xj,\ j\ (\ j\ from\ 1\ to\ 10)$$

Set of constraint:

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

5.2.2. 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 6. 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:

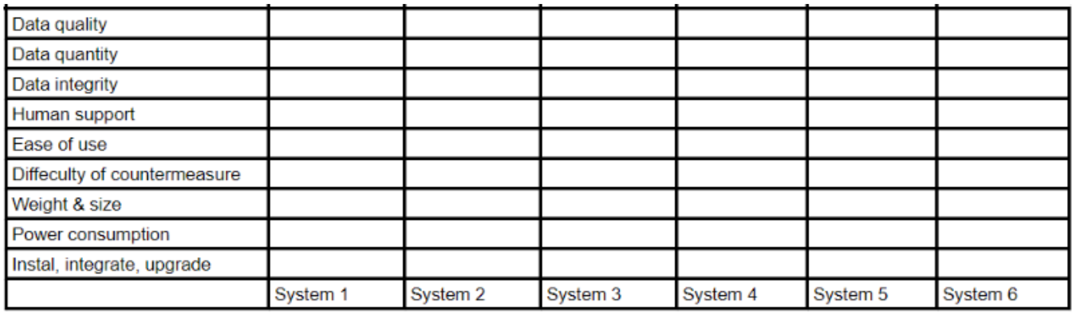
$$\text{maximize} \quad 100x_1 + 60x_2 + 55x_3 + 90x_4 + 90x_5 + 70x_6 + 100x_7$$

Set of constraints:

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

5.3. Results and Conclusion

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.



Data quality						
Data quantity						
Data integrity						
Human support						
Ease of use						
Diffeculty of countermeasure						
Weight & size						
Power consumption						
Instal, integrate, upgrade						
	System 1	System 2	System 3	System 4	System 5	System 6

Table 7. Sensor operational value evaluation used for ILP Model B [Author]

Linear programming optimisation is a valuable tool for complex system design, it can provide insight into a large set of variability, it's a good fit for synchronisation but difficult to implement interoperability, the initial model works well as a proof of concept, the next step to scale up and include more considerations, such as future expectations of the challenges, and what kind of new technologies would be introduced, adding models and increasing the dependencies among them will be critical to the solution, and require a high level of difficulty in model formulation. More Mixed Integer Linear Programming (MILP) techniques to be investigated to have a central and holistic approach to the problem at hand. The proposed system factoring the security needs of the targeted user (Jordan in this case) to have a chance of implementation, a small yet scalable pilot experiment that utilises the current infrastructure of Jordanian border security. For the UAV surveillance solution we found that,

1. Reports on the surveillance operations at the Jordanian border are rather limited, prohibiting baseline for comparison.

2. ILP optimisation models are a good fit for the system design uncertainties, optimising the distribution of ground bases and UAVs along the border.

3. The value of surveillance technology gives the model the main metric to select from multidimensional options, however, the interoperability value is difficult to incorporate.

4. Although not investigated at all in this research, the next improvement to the models is likely to be integrating a blockchain ledger to evaluate the interoperability of potential technologies and multiple UAVs.

5. ILP models are scalable and fit to synchronise between ground fixed & mobile technologies and the UAV technologies.

This chapter showed that both UAV and sensor technologies are effective for perimeter surveillance as of today's performance, at the same time the system is not fully optimised in terms of each particular technology and the potential for interoperability. Based on the results it supports **Hypothesis 1** which posits that “the use of UAVs equipped with advanced sensors and processors can enhance the surveillance of long perimeters, and justify their continued use for border security from a cost-benefit perspective”, and finds no evidence for **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”.

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.

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].

OUTLOOK AND FUTURE WORK

Every sunrise there is a new knowledge mastered by humans, a new technology or technique.

In terms of perimeter security, new challenges are continuously arising as well, and the same technologies and techniques are being used against the security system by many well-resourced criminal groups. The philosophy of this research was to contribute to a framework that connects the security system design aspects and associate each aspect to its historical experience, functionality, means of conduct, and results, mindfully extrapolating from the collective knowledge towards a better way to achieve the task of an impenetrable perimeter, where the objective is to find the optimum security system that can detect intrusions on a stretched perimeter.

This work marks a milestone towards complete expansive perimeter security, the limitations of open information, and lack of universally defined key performance indicators that are specific and measurable left some challenges unsolved, for instance, creating a benchmark dataset to train and test the machine vision algorithms on, the current image registration convert images to grayscale then process it to quantify misregistrations. More investigation is needed to compare the performance using the three separate chromatic bands of red, green, and blue, and also to answer questions such as would a multi-spectral imaging enhance clues detection? and by how much?

The practical optimisation of sensor technologies selection for the anticipated near future development, answering questions such as how new technologies could upgrade the existing ones to achieve the objective result, evaluate the interoperability of potential technologies and multiple UAVs, and how a certain combination of different sensors and techniques working together might differ from another, to overcome the limitation of the ILP models to a few dimensions that determine the overall cost-benefits of a particular technology.

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]. Bejarano, J. P. P. (2020). Digital Hunters: Techno-Territories in the Age of Computational Surveillance. A Peer-Reviewed Journal About, 9(1), 42-52.

[10]. Desporte, G. (2022). Blue hair and pronouns in bio: surveillance of queer BIPOC users and digital identity formation (Doctoral dissertation).

[11]. BlueServo. "About BlueServo." www.blueservo.com, http://www.blueservo.com/about.php.

[12]. 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).

[13]. 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.

[14]. Bunker, R. J., Sullivan, J. P., & Kuhn, D. A. (2021). Use of weaponized consumer drones in Mexican crime war. Small Wars Journal, 70-71.

[15]. Kar, D., & Spanjers, J. (2017). Transnational crime and the developing world. Global Financial Integrity, 53-59.

[16]. Blanding, M. (2015). Workplace stress responsible for up to $190 B in annual US healthcare costs. HBS Working Knowledge; Forbes: Jersey City, NJ, USA.

[17]. Squire, V. (2014). Desert 'trash': Posthumanism, border struggles, and humanitarian politics. Political Geography, 39, 11-21.

[18]. 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.

[19]. 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.

[20]. Office of the Inspector General. (2017). Additional Actions Needed to Better Assess Fencing's Contributions to Operations and Provide Guidance for Identifying Capability Gaps. Southwest Border Security, GAO-17-331

[21]. Ackleson, J. (2005). Border security technologies: Local and regional implications. Review of policy research, 22(2), 137-155.

[22]. Hudspeth, R. A. (2019). Measuring the effectiveness of surveillance technology at the US Southern border (Doctoral dissertation, Monterey, CA; Naval Postgraduate School).

[23]. Koslowski, R., & Schulzke, M. (2018). Drones along borders: Border security UAVs in the United States and the European Union. International Studies Perspectives, 19(4), 305-324.

[24]. Salter, M. B., & Mutlu, C. E. (2012). Psychoanalytic theory and border security. European Journal of Social Theory, 15(2), 179-195.

[25]. Brayne, S. (2022). The banality of surveillance. Surveillance & Society, 20(4), 372-378.

[26]. Karabulut, E., Aras, N., & Altınel, İ. K. (2017). Optimal sensor deployment to increase the security of the maximal breach path in border surveillance. *European Journal of Operational Research*, *259*(1), 19-36.

[27]. Gómez, C., & Green, D. R. (2017). Small unmanned airborne systems to support oil and gas pipeline monitoring and mapping. Arabian Journal of Geosciences, 10, 1-17.

[28]. Yaqoob, T., Arshad, A., Abbas, H., Amjad, M. F., & Shafqat, N. (2019). Framework for calculating return on security investment (ROSI) for security-oriented organizations. Future Generation Computer Systems, 95, 754-763.

[29]. Islamova, O., Hrishko-Dunaievska, V., Biliovskyi, O., Kulagin, O., Hnydiuk, O., & Miroshnichenko, V. (2021). Optimization of training program development for remotely piloted aircraft operators in the sphere of border surveillance.

[30]. Katerynchuk, I., Balendr, A., Komarnytska, O., Islamova, O., Ordynska, I., & Chubina, T. (2021). Training of remotely piloted aircraft operators for border surveillance

in Ukraine based on the European Union standards. Revista Romaneasca pentru Educatie Multidimensionala, 13(3), 134-150.

[31]. Patrick, J. M. (2007). The Economic Cost of Border Security: The Case of the Texas-Mexico Border and the US Visit Program. Borderlands: Comparing Border Security in North America and Europe, 10, 197.

[32]. Bankston, K. S., & Soltani, A. (2013). Tiny constables and the cost of surveillance: Making cents out of United States v. Jones. Yale LJF, 123, 335.

[33]. Ball, K., & Snider, L. (Eds.). (2013). The surveillance-industrial complex: A political economy of surveillance. Routledge.

[34]. Marin, L. (2017). The deployment of drone technology in border surveillance: Between techno-securitization and challenges to privacy and data protection 1. In Surveillance, privacy and security (pp. 107-122). Routledge.

[35]. Walsh, J. P. (2010). From Border Control to Border Care: The Political and Ethical Potential of Surveillance. Surveillance & Society, 8(2), 113-130.

[36]. Faustino, D., & Simões, M. J. (2021). Exploring the Culture of Surveillance: A Qualitative Study in Portugal. TECHNO REVIEW. International Technology, Science and Society Review/Revista Internacional de Tecnología, Ciencia y Sociedad, 10(1), 79-95.

[37]. Gouglidis, A., Green, B., Hutchison, D., Alshawish, A., & de Meer, H. (2018). Surveillance and security: protecting electricity utilities and other critical infrastructures. Energy Informatics, 1, 1-24.

[38]. Kenyon, K. M. (1954). Excavations at Jericho. The Journal of the Royal Anthropological Institute of Great Britain and Ireland, 84(1/2), 103-110.

[39]. Brunet-Jailly, E. (2015). Border Disputes [3 volumes]: A Global Encyclopedia [3 volumes]. Bloomsbury Publishing USA.

[40]. Sharp, J. M. (2023). Jordan: Background and US relations.

[41]. Lee, V., Ang, J., Neo, A., Goh, L. Y., & Liew, N. (2019). Operational vigilance in border security: the Singapore experience. Journal of Police and Criminal Psychology, 34(3), 330-339.

[42]. Chen, C., Li, C., Reniers, G., & Yang, F. (2021). Safety and security of oil and gas pipeline transportation: A systematic analysis of research trends and future needs using WoS. Journal of Cleaner Production, 279, 123583.

[43]. Lewis, T. G. (2019). Critical infrastructure protection in homeland security: defending a networked nation. John Wiley & Sons.

[44]. European Commission. (2011). Assessing the Case for EU Legislation on the Safety and the Possible Impacts of Such an Initiative. Brussels: Directorate General Environment, European Commission.

[45]. Scholl, E., & Westphal, K. (2017). European energy security reimagined: Mapping the risks, challenges and opportunities of changing energy geographies.

[46]. Bridge, G., Özkaynak, B., & Turhan, E. (2018). Energy infrastructure and the fate of the nation: Introduction to special issue. Energy research & social science, 41, 1-11.

[47]. Talarico, L., Sörensen, K., Reniers, G., & Springael, J. (2015). Pipeline security. Securing transportation systems, 281-311.

[48]. Chen, M. Y., & Wu, H. T. (2022). An automatic-identification-system-based vessel security system. IEEE Transactions on Industrial Informatics, 19(1), 870-879.

[49]. Knake, R. K. (2017). A cyberattack on the US power grid. Council on Foreign Relations..

[50]. Luna-Reyes, L. F., Derrick, D. C., Langhals, B., & Nunamaker, J. F. (2013). Collaborative cross-border security infrastructure and systems: Identifying policy,

managerial and technological challenges. International Journal of E-Politics (IJEP), 4(2), 21-38.

[51]. House, W. (2002). US-Canada Smart Border/30 Point Action Plan Update. Office of the Press Secretary, 20021206-1.

[52]. Blum, E., & Barrios, D. (2020). Further Reflection-Surveillance technology boosts border security in Arizona. US Customs and Border Protection, accessed February 18 2021.

[53]. Benjamin, R. (2024). Resisting Borders and Technologies of Violence. Haymarket Books.

[54]. Maphill, map of Irbid-Jordan "http://www.maphill.com/jordan/irbid/maps/gray-map/". Accessed March 04 2023.

[55]. Nesser, P., & Gråtrud, H. (2021). When conflicts do not overspill: The case of Jordan. Perspectives on Politics, 19(2), 492-506.

[56]. 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).

[57]. Mirzaeinia, A., Hassanalian, M., & Lee, K. (2020). Drones for borders surveillance: autonomous battery maintenance station and replacement for multirotor drones. In AIAA Scitech 2020 Forum (p. 0062).

[58]. Szabolcsi, R. (2014). A new approach of certification of the airworthiness of the UAV automatic flight control systems. Land Forces Academy Review, 19(4), 423.

[59]. Fahlstrom, P. G., Gleason, T. J., & Sadraey, M. H. (2022). Introduction to UAV systems. John Wiley & Sons.

[60]. Ducard, G. J., & Allenspach, M. (2021). Review of designs and flight control techniques of hybrid and convertible VTOL UAVs. Aerospace Science and Technology, 118, 107035.

[61]. Fendji, J. L. E. K., Bayaola, I. K., Thron, C., Fendji, M. D., & Förster, A. (2020). Cost-effective placement of recharging stations in drone path planning for surveillance missions on large farms. Symmetry, 12(10), 1661.

[62]. Snow, C. Making Sense of Drones. "http://droneanalyst.com/2014/02/06/making-sense-of-drones". Accessed March 20 2022.

[63]. Rajashekara, K. (2013). Present status and future trends in electric vehicle propulsion technologies. IEEE journal of emerging and selected topics in power electronics, 1(1), 3-10.

[64]. Hassanalian, M., Radmanesh, M., & Sedaghat, A. (2014). Increasing flight endurance of MAVs using multiple quantum well solar cells. International Journal of Aeronautical and Space Sciences, 15(2), 212-217.

[65]. Joshi, D., Deb, D., & Muyeen, S. M. (2022). Comprehensive Review on Electric Propulsion System of Unmanned Aerial Vehicles. Frontiers in Energy Research, 10, 752012.

[66]. Team DRONEII.com. Drone Energy Sources – Pushing the Boundaries of Electric Flight "https://droneii.com/drone-energy-sources" Accessed July 12 2021.

[67]. Yao, Z., & Wu, S. (2019). Intermittent gliding flight control design and verification of a morphing unmanned aerial vehicle. IEEE Access, 7, 40991-41005.

[68]. Husain, U., & Rahman, A. (2022). Global drone revolution and related regulatory framework: A critical review. Journal of Statistics and Management Systems, 25(5), 1161-1173.

[69]. Statista Research Department, Global unmanned aerial vehicle market segmentation 2020 "https://www.statista.com/statistics/431717/global-uav-market-size-by-application/" Accessed May 01 2022.

[70]. Szabolcsi, R. (2018). Robust Control System Design for Small UAV Using H2-Optimization. Land Forces Academy Review, 23(2), 151-159.

[71]. Yu, X. (2015). Sense and avoid technologies with applications to unmanned aircraft systems: Review and prospects. Progress in Aerospace Sciences, 74, 152-166

[72]. Zeng, Y., Zhang, R., & Lim, T. J. (2016). Wireless communications with unmanned aerial vehicles: Opportunities and challenges. IEEE Communications magazine, 54(5), 36-42.

[73]. Loukinas, P. (2022). Drones for border surveillance: Multipurpose use, uncertainty and challenges at EU borders. Geopolitics, 27(1), 89-112.

[74]. Nassi, B., Bitton, R., Masuoka, R., Shabtai, A., & Elovici, Y. (2021, May). SoK: Security and privacy in the age of commercial drones. In 2021 IEEE Symposium on Security and Privacy (SP) (pp. 1434-1451). IEEE.

[75]. Djuyandi, Y., Husin, L. H., Ummah, M., Iriansyah, M. N., & Ramadhani, R. (2023). Re-Defining Threat To National Defence: Case Study Of Indonesia-Malaysia Border Dispute In West Kalimantan. Journal of Namibian Studies: History Politics Culture, 33, 851-865.

[76]. Geddes, A., Hadj-Abdou, L., & Brumat, L. (2020). Migration and mobility in the European Union. Bloomsbury Publishing.

[77]. Frontex Risk Analysis Unit, regular overview of irregular migration at the EU's external borders "https://www.frontex.europa.eu/assets/Publications/Risk_Analysis/FRAN_Q2_2017.pdf"

[78]. Hartmann, K., & Steup, C. (2013, June). The vulnerability of UAVs to cyber attacks-An approach to the risk assessment. In 2013 5th international conference on cyber conflict (CYCON 2013) (pp. 1-23). IEEE.

[79]. Szabolcsi, R. (2020). 3D flight path planning for multirotor UAV. Review of the Air Force Academy, (1), 5-16.

[80]. Nguyen, H. P. D., & Nguyen, D. D. (2021). Drone application in smart cities: The general overview of security vulnerabilities and countermeasures for data communication. Development and Future of Internet of Drones (IoD): Insights, Trends and Road Ahead, 185-210.

[81]. Szabolcsi, R. (2013). Analysis Of Robustness Of The Uav Stability Augmentation Systems. Scientific Research & Education in the Air Force-AFASES, 2.

[82]. Szabolcsi, R. (2018). Robust LQG controller design for the small unmanned aerial vehicle. Review of the Air Force Academy, (1), 31-38.

[83]. Khan, M., Heurtefeux, K., Mohamed, A., Harras, K. A., & Hassan, M. M. (2017). Mobile target coverage and tracking on drone-be-gone UAV cyber-physical testbed. IEEE Systems Journal, 12(4), 3485-3496.

[84]. Tang, A. C. (2021). A review on cybersecurity vulnerabilities for urban air mobility. In AIAA Scitech 2021 Forum (p. 0773). [Original source: https://studycrumb.com/alphabetizer]

[85]. Schmidt, D., Radke, K., Camtepe, S., Foo, E., & Ren, M. (2016). A survey and analysis of the GNSS spoofing threat and countermeasures. ACM Computing Surveys (CSUR), 48(4), 1-31.

[86]. Ralegankar, V. K., Bagul, J., Thakkar, B., Gupta, R., Tanwar, S., Sharma, G., & Davidson, I. E. (2021). Quantum Cryptography-as-a-Service for Secure UAV Communication: Applications, Challenges, and Case Study. IEEE Access, 10, 1475-1492.

[87]. Greer, C., Burns, M., Wollman, D., & Griffor, E. (2019) Cyber-Physical Systems and Internet of Things. National Institute of Standards and Technology, US Department of

Commerce. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1900-202.pdf

[88]. Gupta, N., Tiwari, A., Bukkapatnam, S. T., & Karri, R. (2020). Additive manufacturing cyber-physical system: Supply chain cybersecurity and risks. IEEE Access, 8, 47322-47333.

[89]. Cheung, K. F., Bell, M. G., & Bhattacharjya, J. (2021). Cybersecurity in logistics and supply chain management: An overview and future research directions. Transportation Research Part E: Logistics and Transportation Review, 146, 102217.

[90]. Iqbal, S. (2021, January). A study on UAV operating system security and future research challenges. In 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 0759-0765). IEEE.

[91]. Zhao, N., Yang, X., Ren, A., Zhang, Z., Zhao, W., Hu, F., ... & Abolhasan, M. (2018). Antenna and propagation considerations for amateur UAV monitoring. IEEE Access, 6, 28001-28007. [Original source: https://studycrumb.com/alphabetizer]

[92]. Mohammadi, A., Rahmati, M., & Malik, H. (2022). Location-Aware Beamforming for MIMO-Enabled UAV Communications: An Unknown Input Observer Approach. IEEE Sensors Journal, 22(8), 8206-8215.

[93]. Jacobsen, R. H., & Marandi, A. (2021, November). Security Threats Analysis of the Unmanned Aerial Vehicle System. In MILCOM 2021-2021 IEEE Military Communications Conference (MILCOM) (pp. 316-322). IEEE.

[94]. Semenov, S., Voloshyn, D., Lymarenko, V., Semenova, A., & Davydov, V. (2019, June). Method of UAVs Quasi-Autonomous Positioning in the External Cyber Attacks Conditions. In 2019 10th International Conference on Dependable Systems, Services and Technologies (DESSERT) (pp. 149-153). IEEE.

[95]. Hu, J., Ma, D., Liu, C., Shi, Z., Yan, H., & Hu, C. (2019). Network security situation prediction based on MR-SVM. IEEE Access, 7, 130937-130945.

[96]. Araújo, R., Pinto, A., & Pinto, P. (2021, June). A performance assessment of free-to-use vulnerability scanners-revisited. In IFIP International Conference on ICT Systems Security and Privacy Protection (pp. 53-65). Springer, Cham.

[97]. 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.

[98]. Khan, S. Z., Mohsin, M., & Iqbal, W. (2021). On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions. PeerJ Computer Science, 7, e507.

[99]. Ma, C., Yang, J., Chen, J., Qu, Z., & Zhou, C. (2020). Effects of a navigation spoofing signal on a receiver loop and a UAV spoofing approach. GPS Solutions, 24(3), 1-13.

[100]. Hamurcu, M., & Eren, T. (2020). Selection of unmanned aerial vehicles by using multicriteria decision-making for defense. Journal of Mathematics, 2020.

[101]. Lin, K. P., & Hung, K. C. (2011). An efficient fuzzy weighted average algorithm for the military UAV selecting under group decision-making. Knowledge-Based Systems, 24(6), 877-889.

[102]. Alex, A. (2022, July 15). 8 ways to increase your drone's range. Phantomangel. https://phantomangel.rocks/8-ways-to-increase-your-drones-range.html

[103]. Daudelin, M. (2022, July 11) ‘Nessus Scan Report’,. Tenable. https://www.tenable.com/sites/all/themes/tenablefourteen/img/nessus/live-results.jpg

[104]. Driscoll, K. (2018, April). Lightweight crypto for lightweight unmanned arial systems. In 2018 Integrated Communications, Navigation, Surveillance Conference (ICNS) (pp. 1-15). IEEE.

[105]. 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

[106]. Liu, Y., Li, S., Fu, Q., & Liu, Z. (2018). Impact assessment of GNSS spoofing attacks on INS/GNSS integrated navigation system. Sensors, 18(5), 1433.

[107]. Jing, H., Gao, Y., Shahbeigi, S., & Dianati, M. (2022). Integrity Monitoring of GNSS/INS Based Positioning Systems for Autonomous Vehicles: State-of-the-Art and Open Challenges. IEEE Transactions on Intelligent Transportation Systems.

[108]. Park, K., Kang, J., Arjmandi, Z., Shahbazi, M., & Sohn, G. (2020). Multilateration Under Flip Ambiguity For Uav Positioning Using Ultrawide-Band. ISPRS Annals of Photogrammetry, Remote Sensing & Spatial Information Sciences, 5(1).

[109]. Wang, P., R. Krishnamurti, and K. Gupta, 2010. Generalized watchman route problem with discrete view cost, International Journal of Computational Geometry & Applications, 20(02):119–146.

[110]. British Broadcasting Corporation BBC. Saudi oil attacks: Images show detail of damage "https://www.bbc.com/news/world-middle-east-49718975" Accessed April 26 2020.

[111]. American Fence Company Des Moines – Ameristar Ornamental Fencing, Stalwart IS crash test "https://desmoinesfencecompany.com/products/k-rated-vehicle-restraint-systems/stalwart-is-crash-test/" Accessed April 26 2020.

[112]. United Nations Office on Drugs and Crime, Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes: Research Report (Vienna, October 2011). Available from www.unodc.org/documents/data-and-analysis/Studies/Illicitfinancial_flows_2011_web.pdf.

[113]. Romsom, E. (2022). Global oil theft: impact and policy responses (No. 2022/16). WIDER Working Paper.

[114]. Alarm, Victoria. “Steveston Harbour Wharf Fire Security Camera Footage.” YouTube, 15 August 2017, https://www.youtube.com/watch?v=Oe573lToJQE. Accessed 25 June 2023.

[115]. TOTAL Group, 2019. Integrating climate into our strategy [www.total.com document]. URL. https://www.total.com/sites/default/files/atoms/files/total_rapport_climat_2019_en.pdf#page=30 Accessed 11 August 2023.

[116]. Cellini, A., Blasioli, S., Biondi, E., Bertaccini, A., Braschi, I., & Spinelli, F. (2017). Potential applications and limitations of electronic nose devices for plant disease diagnosis. Sensors, 17(11), 2596.

[117]. Haas, P. Y., Balistreri, C., Pontelandolfo, P., Triscone, G., Pekoz, H., & Pignatiello, A. (2014). Development of an unmanned aerial vehicle UAV for air quality measurement in urban areas. In 32nd AIAA Applied Aerodynamics Conference (p. 2272).

[118]. Szabolcsi, R. (2020). Flight path planning for small UAV low altitude flights. Land Forces Academy Review, 25(2), 159-167.

[119]. Miller, A., Shah, M., & Harper, D. (2008, May). Landing a UAV on a runway using image registration. In 2008 IEEE International Conference on Robotics and Automation (pp. 182-187). IEEE.

[120]. Wang, X., Kealy, A., Li, W., Jelfs, B., Gilliam, C., Le May, S., & Moran, B. (2021). Toward autonomous uav localization via aerial image registration. Electronics, 10(4), 435.

[121]. Vakalopoulou, M., Christodoulidis, S., Sahasrabudhe, M., Mougiakakou, S., & Paragios, N. (2019, July). Image registration of satellite imagery with deep convolutional

neural networks. In IGARSS 2019-2019 IEEE International Geoscience and Remote Sensing Symposium (pp. 4939-4942). IEEE.

[122]. Li, Z., & Leung, H. (2007, July). Contour-based multisensor image registration with rigid transformation. In 2007 10th International Conference on Information Fusion (pp. 1-7). IEEE.

[123]. Crazzolara, C., Ebner, M., Platis, A., Miranda, T., Bange, J., & Junginger, A. (2019). A new multicopter-based unmanned aerial system for pollen and spores collection in the atmospheric boundary layer. Atmospheric Measurement Techniques, 12(3), 1581-1598.

[124]. Luo, B., Meng, Q. H., Wang, J. Y., & Zeng, M. (2017). A flying odor compass to autonomously locate the gas source. IEEE Transactions on Instrumentation and Measurement, 67(1), 137-149.

[125]. Burgués, J., Hernández, V., Lilienthal, A. J., & Marco, S. (2019). Smelling nano aerial vehicle for gas source localization and mapping. Sensors, 19(3), 478.

[126]. Niedzielski, T., Jurecka, M., Miziński, B., Pawul, W., & Motyl, T. (2021). First successful rescue of a lost person using the human detection system: A case study from Beskid Niski (SE Poland). Remote Sensing, 13(23), 4903.

[127]. Szabolcsi, R. (2014). A new approach of certification of the airworthiness of the UAV automatic flight control systems. Land Forces Academy Review, 19(4), 423.

[128]. Haddal, C. C., & Gertler, J. (2010). Homeland security: Unmanned aerial vehicles and border surveillance.

[129]. Zoph, Barret, Vijay Vasudevan, Jonathon Shlens, and Quoc V. Le. “Learning Transferable Architectures for Scalable Image Recognition.” Preprint, submitted in 2017. https://doi.org/10.48550/ARXIV.1707.07012.

[130]. Van Maanen, H. Geurproef dient niet meer als bewijs in strafzaak. Volkskrant 2011-04-22.

[131]. de Lacy Costello, B., Amann, A., Al-Kateb, H., Flynn, C., Filipiak, W., Khalid, T., ... & Ratcliffe, N. M. (2014). A review of the volatiles from the healthy human body. Journal of breath research, 8(1), 014001.

[132]. Tavares, D. S., Mesquita, P. R., Salgado, V. R., Rodrigues, F. D. M., Miranda, J. C., Barral-Netto, M., ... & Barral, A. (2019). Determination and profiling of human skin odors using hair samples. Molecules, 24(16), 2964.

[133]. Wongchoosuk, C., Lutz, M., & Kerdcharoen, T. (2009). Detection and classification of human body odor using an electronic nose. Sensors, 9(9), 7234-7249.

[134]. Staymates, M. E. et al. Biomimetic Sniffing Improves the Detection Performance of a 3D Printed Nose of a Dog and a Commercial Trace Vapor Detector. Sci. Rep. 6, 36876; doi: 10.1038/srep36876 (2016).

[135]. Brunhuber, Kim. "Why U.S. Border Patrol only catches 54% of the people crossing illegally from Mexico." https://www.cbc.ca/news/world/united-states-border-patrol-1.3796371, 2016. Accessed 18 December 2023.

[136]. Army Unmanned Aircraft Systems Center Of Excellence Fort Rucker AL. (2010). US Army Unmanned Aircraft Systems Roadmap 2010-2035: Eyes of the Army.

[137]. Al-Bilbisi, H. (2013). Topography and morphology. Atlas of Jordan: History, territories and society, 42-46.

[138]. Northrop Grumman Electro-optical/infrared spot collection mode vs wide 10 km swath search mode "https://www.uvs-info.com/index.php?option=com_docman&task=doc_view&gid=8149&Itemid=144" Accessed January 19 2020.

[139]. Chen, Z. Y., Gogoi, A., Lee, S. Y., Tsai-Lin, Y., Yi, P. W., Lu, M. K., ... & Kao, F. J. (2018). Coherent narrow-band light source for miniature endoscopes. IEEE Journal of Selected Topics in Quantum Electronics, 25(1), 1-7.

[140]. Arnon, S. (Ed.). (2015). Visible light communication. Cambridge University Press.

[141]. GHERDEVICH, D., BARSANTI, S. G., & DEGRASSI, D. Historic and archaeological itineraries for the discovery of Friuli during the Lombard period.

[142]. Rizo-Maestre, C., González-Avilés, Á., Galiano-Garrigós, A., Andújar-Montoya, M. D., & Puchol-García, J. A. (2020). UAV+ BIM: Incorporation of photogrammetric techniques in architectural projects with building information modeling versus classical work processes. Remote Sensing, 12(14), 2329.

[143]. Morales-Rodríguez, Marissa E., Larry R. Senesac, Thomas Thundat, Michael K. Rafailov, and Panos G. Datskos. "Standoff imaging of chemicals using IR spectroscopy." In Micro-and Nanotechnology Sensors, Systems, and Applications III, vol. 8031, pp. 686-693. SPIE, 2011.

[144]. Petersson, H., & Gustafsson, D. (2016, October). Multi-spectral texture analysis for IED detection. In Electro-Optical Remote Sensing X (Vol. 9988, pp. 206-219). SPIE.

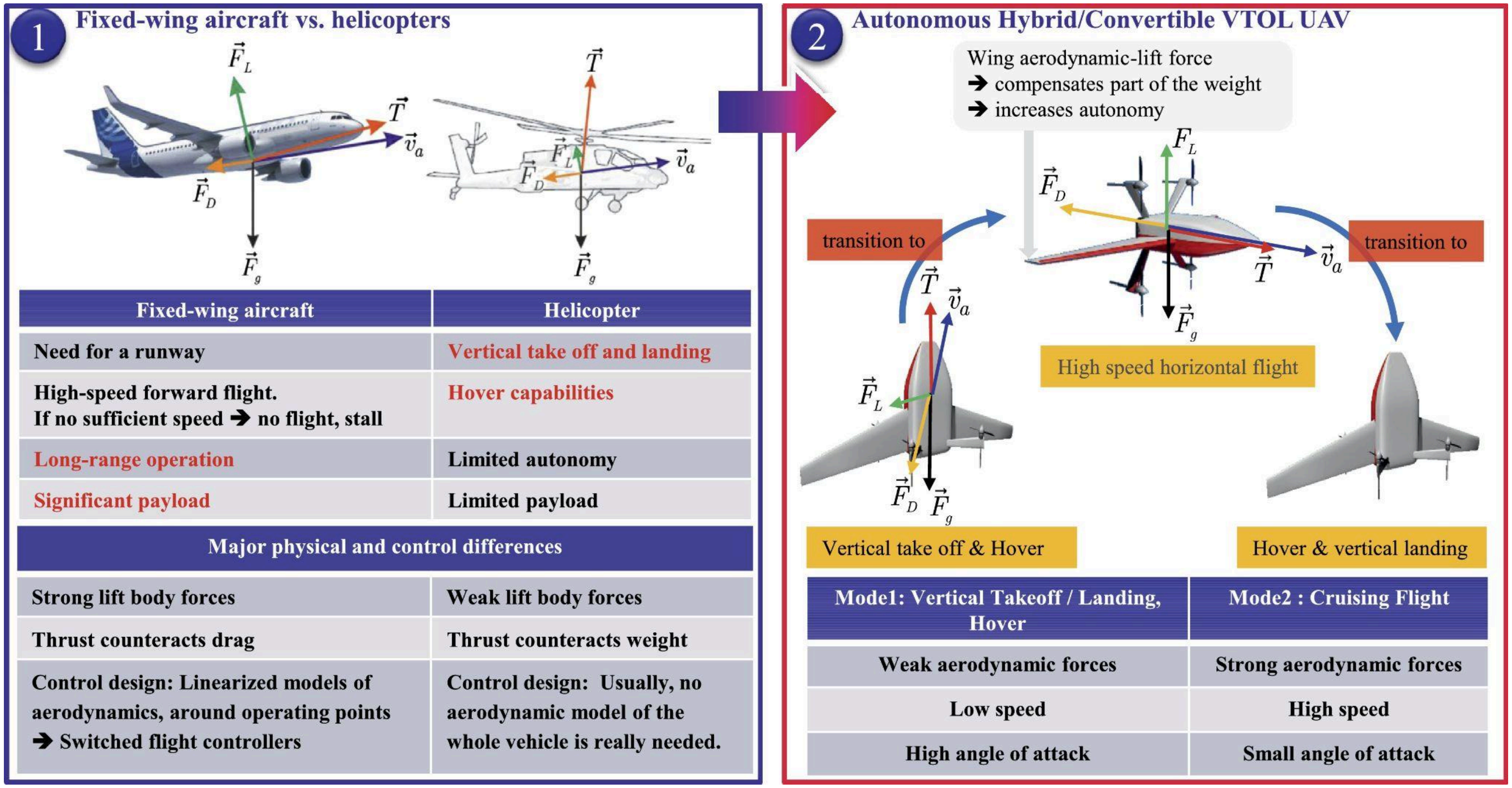
[145]. Tomasik, J. (2021). Drones–challenges and chances concerning the security environment. Наукові заходи Юридичного факультету Західноукраїнського національного університету, 167-180.

[146]. Meyer, Franz. "Spaceborne Synthetic Aperture Radar – Principles, Data Access, and Basic Processing Techniques." SAR Handbook: Comprehensive Methodologies for Forest Monitoring and Biomass Estimation. Eds. Flores, A., Herndon, K., Thapa, R., Cherrington, E. NASA. 2019.

[147]. Army Unmanned Aircraft Systems Center Of Excellence Fort Rucker AL. (2010). US Army Unmanned Aircraft Systems Roadmap 2010-2035: Eyes of the Army.

[148]. Forum user, mourad27. (n.d.). Armee jordanienne / Jordanian Armed Forces. Far-Maroc Forum. https://far-maroc.forumpro.fr/t455p250-armee-jordanienne-jordanian-armed-forces.

Appendix (Larger size Figures 4, 6, 9, 14, 34, 37, 41)



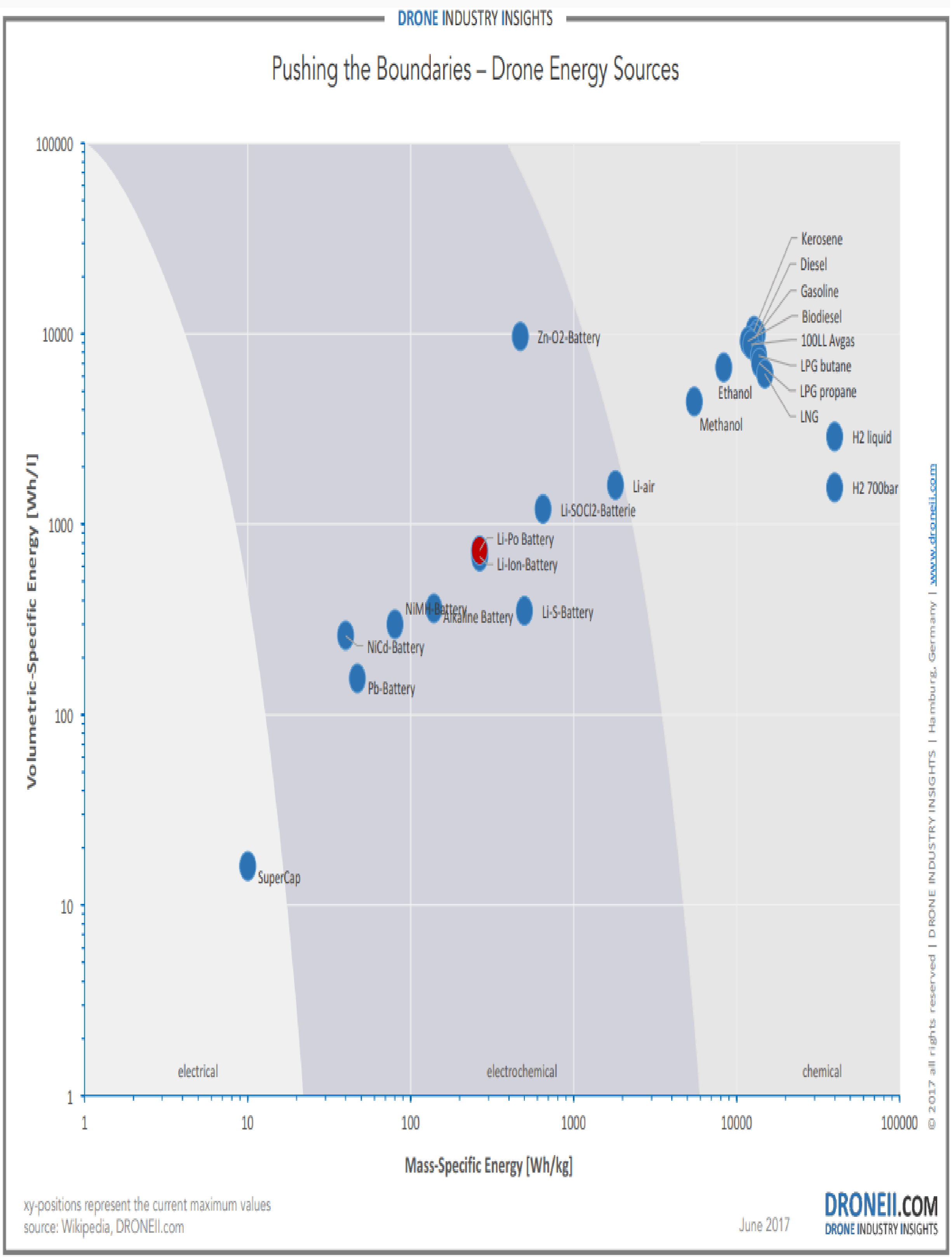
1
Fixed-wing aircraft vs. helicopters
$\vec{F}_L$
$\vec{T}$
$\vec{v}_a$
$\vec{F}_D$
$\vec{F}_g$
2
Autonomous Hybrid/Convertible VTOL UAV
transition to
Vertical take off & Hover
High speed horizontal flight
Hover & vertical landing

Wing aerodynamic-lift force
➔ compensates part of the weight
➔ increases autonomy

Fixed-wing aircraft	Helicopter
Need for a runway	Vertical take off and landing
High-speed forward flight. If no sufficient speed ➔ no flight, stall	Hover capabilities
Long-range operation	Limited autonomy
Significant payload	Limited payload

Major physical and control differences	
Strong lift body forces	Weak lift body forces
Thrust counteracts drag	Thrust counteracts weight
Control design: Linearized models of aerodynamics, around operating points ➔ Switched flight controllers	Control design: Usually, no aerodynamic model of the whole vehicle is really needed.

Mode1: Vertical Takeoff / Landing, Hover	Mode2 : Cruising Flight
Weak aerodynamic forces	Strong aerodynamic forces
Low speed	High speed
High angle of attack	Small angle of attack



DRONE INDUSTRY INSIGHTS

Pushing the Boundaries – Drone Energy Sources

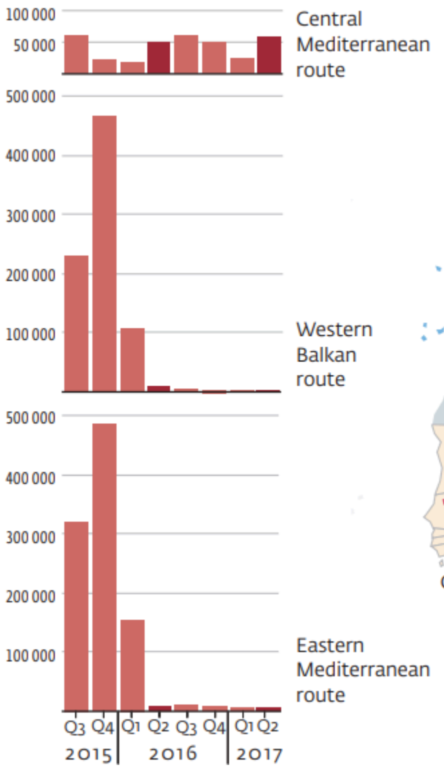
xy-positions represent the current maximum values
source: Wikipedia, DRONEII.com

June 2017

Trend

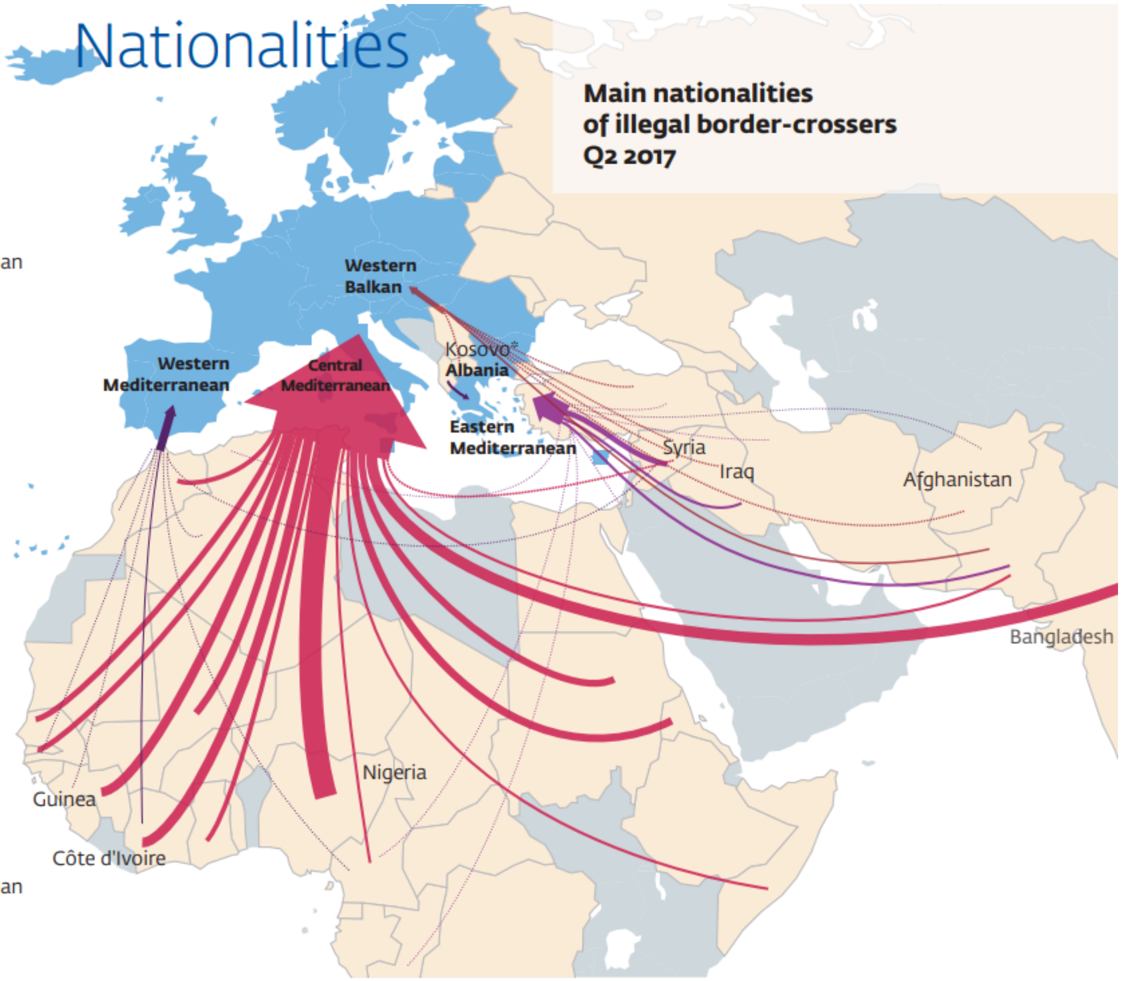
Quarterly detections of illegal border-crossing, 2015–2017

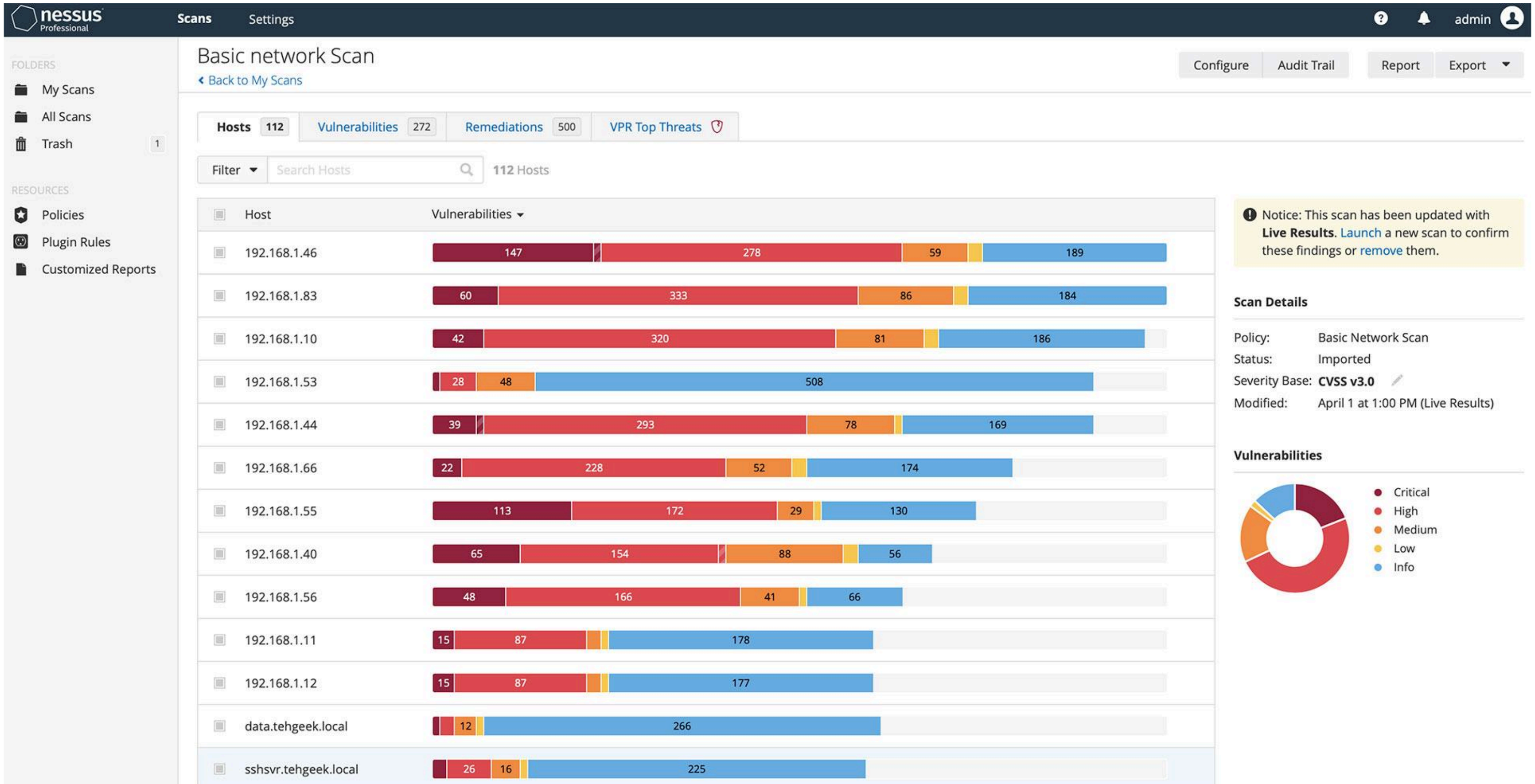
Number



Nationalities

Main nationalities of illegal border-crossers Q2 2017





Basic network Scan

‹ Back to My Scans

112 Hosts

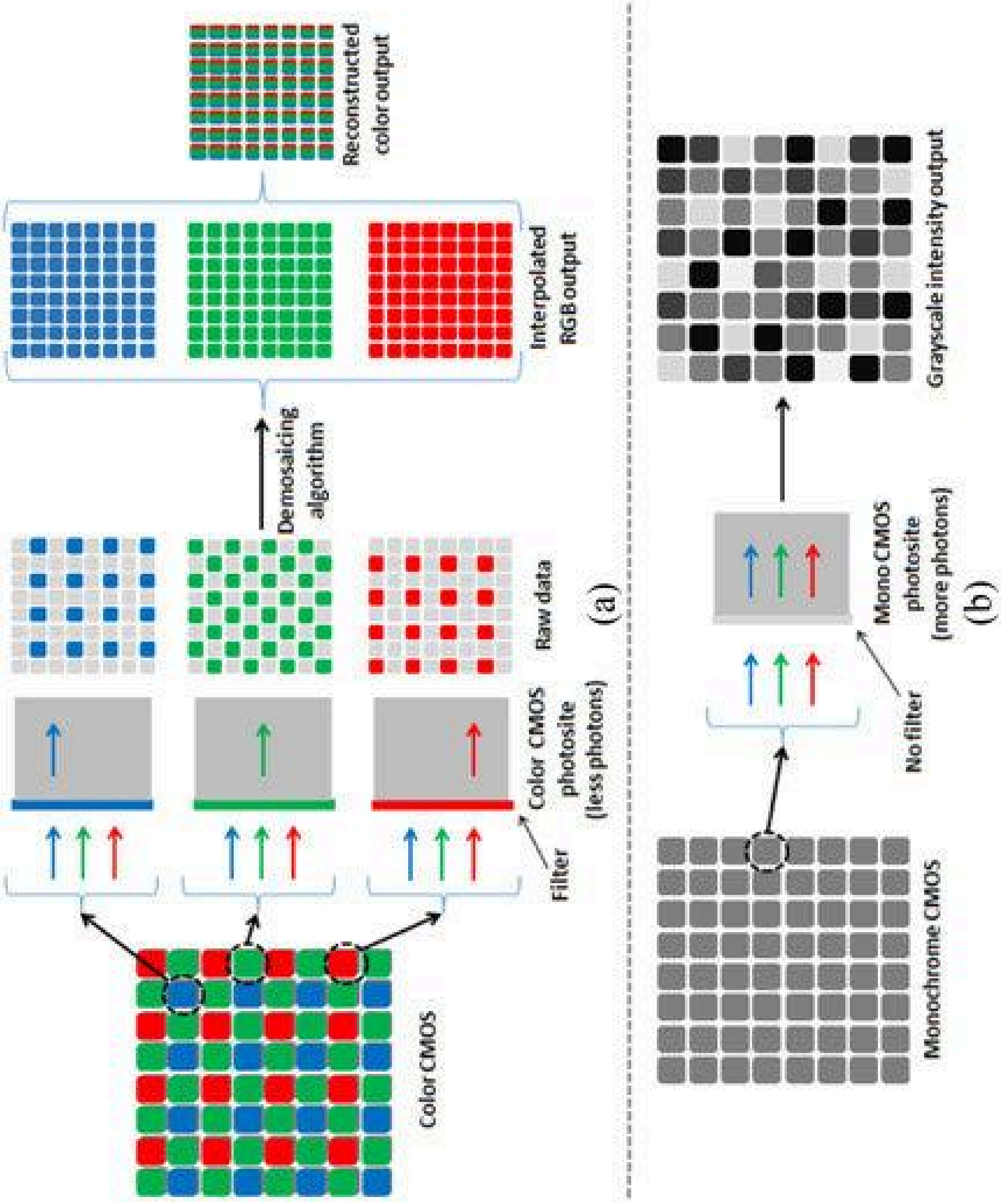
Host	Vulnerabilities
192.168.1.46	147 278 59 189
192.168.1.83	60 333 86 184
192.168.1.10	42 320 81 186
192.168.1.53	28 48 508
192.168.1.44	39 293 78 169
192.168.1.66	22 228 52 174
192.168.1.55	113 172 29 130
192.168.1.40	65 154 88 56
192.168.1.56	48 166 41 66
192.168.1.11	15 87 178
192.168.1.12	15 87 177
data.tehgeek.local	12 266
sshsvr.tehgeek.local	26 16 225

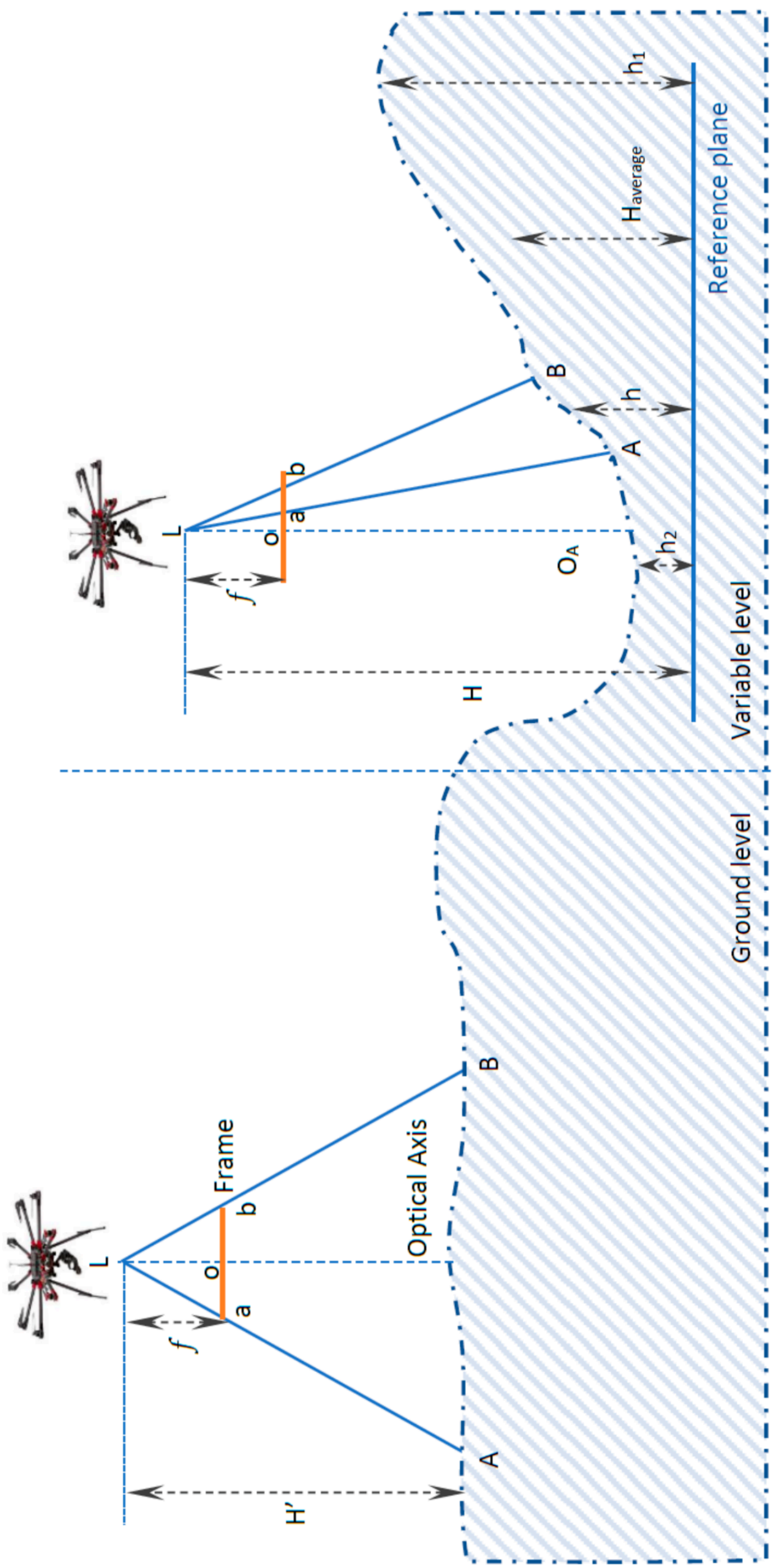
Notice: This scan has been updated with **Live Results.** Launch a new scan to confirm these findings or remove them.

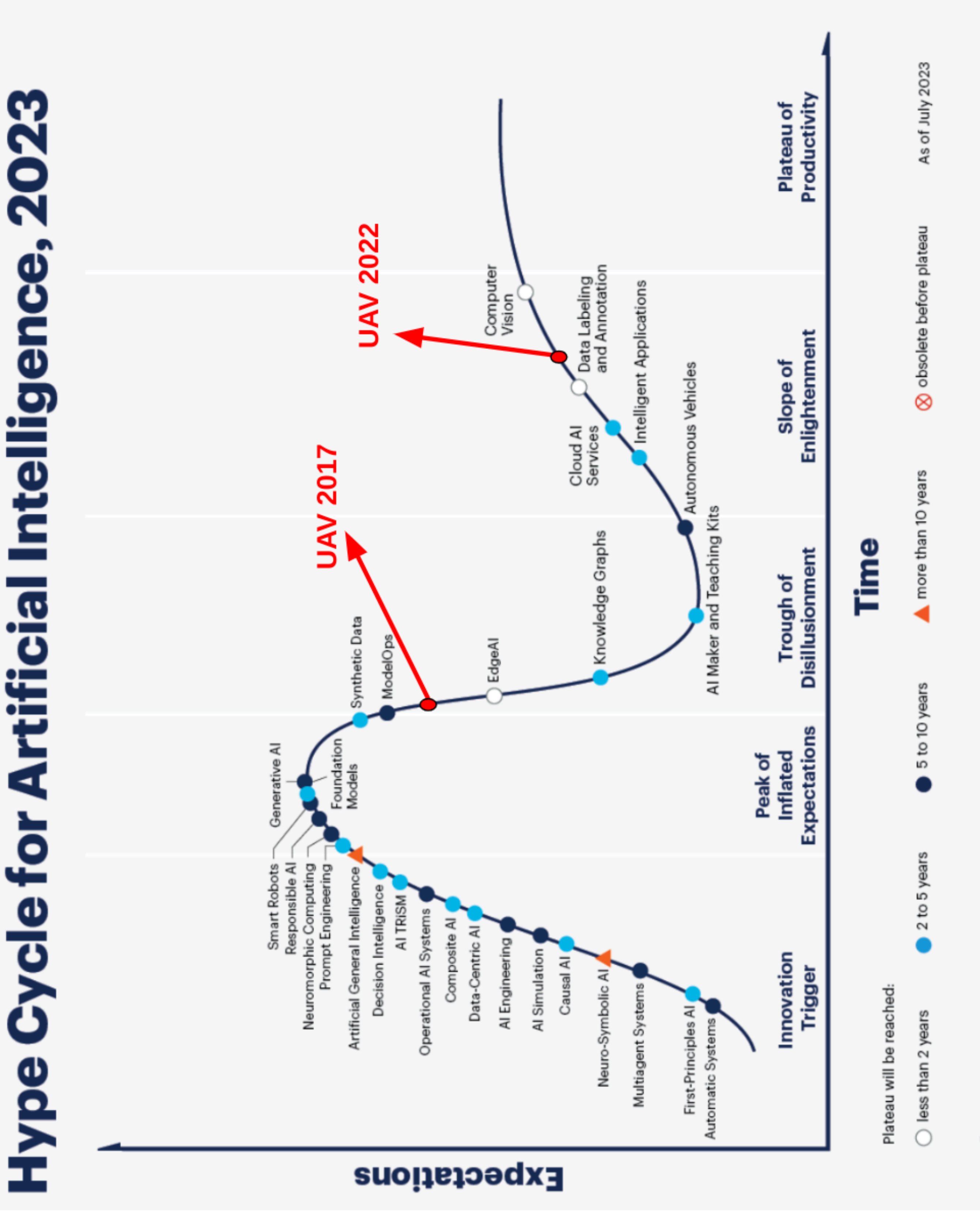
Scan Details

Policy: Basic Network Scan
Status: Imported
Severity Base: **CVSS v3.0**
Modified: April 1 at 1:00 PM (Live Results)

Vulnerabilities


Color CMOS
Filter
Color CMOS photosite (less photons)
Raw data
Demosaicing algorithm
Interpolated RGB output
Reconstructed color output
(a)
Monochrome CMOS
No filter
Mono CMOS photosite (more photons)
(b)
Grayscale intensity output


L
f
a
o
b
Frame
Optical Axis
A
B
H'
Ground level
L
f
o
a
b
O_A
A
B
h
h_2
H
Variable level
H_average
h_1
Reference plane


Hype Cycle for Artificial Intelligence, 2023
Expectations
Smart Robots
Responsible AI
Neuromorphic Computing
Prompt Engineering
Artificial General Intelligence
Decision Intelligence
AI TRiSM
Operational AI Systems
Composite AI
Data-Centric AI
AI Engineering
AI Simulation
Causal AI
Neuro-Symbolic AI
Multiagent Systems
First-Principles AI
Automatic Systems
Generative AI
Foundation Models
Synthetic Data
ModelOps
EdgeAI
Knowledge Graphs
AI Maker and Teaching Kits
Autonomous Vehicles
Cloud AI Services
Intelligent Applications
Data Labeling and Annotation
Computer Vision
UAV 2017
UAV 2022
Innovation Trigger
Peak of Inflated Expectations
Trough of Disillusionment
Slope of Enlightenment
Plateau of Productivity
Time
Plateau will be reached:
○ less than 2 years
● 2 to 5 years
● 5 to 10 years
▲ more than 10 years
⊗ obsolete before plateau
As of July 2023