MS-E2177 - Seminar on Case Studies in Operations Research

Cost-Efficient Defence Against Unmanned Aerial Systems

Final report

Case Group Patria

Ahti Korhonen
Joona Lindell (Project Manager)
Petra Lähteenmäki
Samuel Toivonen

May 14, 2025

Contents

1 Introduction

Patria is a government-owned Finnish defence, security, and aviation company specializing in armored vehicles, weapon systems, and aerospace solutions. It provides advanced defence technology, life-cycle support, and training services for military and security forces worldwide.

The rapid development of unmanned aerial systems (UAS) has transformed modern warfare and security dynamics. Use of commercial drones in modern warfare has led to an asymmetric situation where the resulting threats can inflict damage on high-value military targets. This cost imbalance necessitates the development of countermeasures that provide effective defence while maintaining economic viability.

Patria is interested in discovering cost-effective defence solutions against unmanned aerial systems, considering the Finnish operational environment. The Finnish environment poses unique opportunities and constraints due to its four-season climate, dense forests, and vast, sparsely populated areas. The aim of this project is to identify balanced countermeasures that optimize spatial coverage, resource allocation, and operational effectiveness, particularly against tactical-level threats such as small drones with limited range and payload.

1.1 Objectives

The central objective of this project is to create a simulation framework which may be used to study and identify cost-effective and operationally viable methods of defending a company-sized troop in Finnish environment against threats posed by small unmanned aerial systems. The model should be simple enough such that further developments and additions may be built on top the project to further develop the model.

To achieve this objective, this project employs a Monte Carlo based approach to model different defensive configurations and evaluate their effectiveness. Each defensive scenario is parametrized using probabilistic detection and interception models.

2 Literature Review

The increasing accessibility of unmanned aerial systems has spurred concerns about their potential misuse in both military and civilian environments. This has led to the development of Counter-Unmanned Aerial Vehicle Systems (counter-UAV systems) designed to detect, track, and neutralize rogue UAVs. Kang et al. (2020) emphasize that the proliferation of small and micro drones, in particular, presents new challenges to conventional air defence systems, which are typically designed to detect and engage larger, high-altitude aircraft.

The architecture of a counter-UAV system is typically structured around three components: detection, identification, and mitigation (Chauhan et al., 2025). As the authors describe, detection forms the foundation of the system and enables the estimation of key parameters, such as location of the threat. Once a potential threat is detected and possibly identified, appropriate mitigation actions can be deployed.

In military doctrine, the process of responding to a threat is often conceptualized using the F2T2EA kill chain — comprising the stages of Find, Fix, Track, Target, Engage, and Assess. In the context of counter-UAV systems, the F2T2EA model is used to guide the detection, tracking, and interception of incoming UAV threats.

2.1 Detection and Mitigation Technologies for UAVs

Contemporary counter-UAV systems are typically classified into ground-based and aerial systems based on their deployment platform (Brooks et al., 2019). Over 90 percent of counter-UAV technologies are ground-based, either deployed as stationary systems or mounted on mobile platforms (Kang et al., 2020). Among these, fixed ground installations are the most prevalent, with jamming technologies representing the most widely adopted form of countermeasure.

Park et al. (2021) provide an overview of the most commonly employed technologies in counter-UAV systems, such as radars, acoustic sensors and laser range finders. The performance of various methods is assessed under different conditions, emphasizing the importance of selecting appropriate technologies based on specific scenarios. They also suggest that in order to address the inherent limitations of individual sensors the use of hybrid detection systems that integrate multiple complementary technologies can provide more reliable performance and improve overall detection accuracy.

A simulation framework developed by Besada et al. (2021) characterizes each sensor using probabilistic models of detections and measurement error. The models incorporate distance-dependent detection probabilities which are used to estimate the sensor effectiveness over a range of operating conditions. Brewczyński et al. (2024) introduce a methodology for assessing the effectiveness counter-UAV systems. The authors propose a multi-criteria decision analysis framework that incorporates both technical specifications and environmental considerations.

Kashi et al. (2024) present a review of drone detection systems using a scenario based, system engineering approach. Their methodology evaluates various technologies across scenarios including urban environments and critical infrastructure. The study highlights the impact of environmental conditions, such as line-of-sight obstruction and noise levels, on system performance.

2.2 Simulation-Based Approaches for Counter-UAV Strategy Development

Simulations are widely used in the development and evaluation of counter-UAV strategies, offering a flexible and cost-effective means of modeling aerial defence scenarios. Karadeniz et al. (2024) introduce a game-based simulation environment to examine aerial defence tactics against drone swarms. The platform enables testing of multiple types of countermeasure systems. Their

findings demonstrate that simulation-based games can replicate threat environments and serve as tools for assessing the viability counter-UAV solutions.

Similarly, simulations are used to evaluate system-level responses to UAV attacks in the work of Fangzi et al. (2024), who applied a model-based systems engineering approach to the design of air defence against UAV swarms. Their simulation framework incorporates physical systems and operational flows as well as organizational models.

A systems-level simulation is also adopted by Tan et al. (2021), who analyze the counter-UAV kill chain in operational environments. The study focuses on modeling the interdependencies between detection, identification and neutralization. With regards to the F2T2EA kill chain, the authors suggest that the kill chain can be simplified to focus only on the detection and interception phases.

Another line of research explores simulation techniques grounded in adversarial risk analysis (ARA) to account for strategic interactions under uncertainty in counter-UAV scenarios. Roponen et al. (2020) present a simulation framework based on ARA to support defensive decision-making in situations where the attacker's preferences are only partially known. The defender evaluates countermeasure portfolios against UAV threats and Monte Carlo simulations are used to assess detection probabilities, weapon effectiveness and potential damage outcomes.

3 Modeling

3.1 Threat Characterization

The simulation model distinguishes between two primary categories of UAVs: multicopters and small fixed-wing UAVs. These two threat types differ in terms of operational characteristics and the risk they pose to ground assets.

Multicopters are characterized by their low manufacturing cost and their relatively low speed. Because they are inexpensive and agile, they are assumed to constitute the majority of the threat actors in the simulation. However, their ability to cause damage to ground assets is limited, with a hit probability of 50% upon reaching the asset.

In comparison, fixed wing drones represent a more advanced threat. These drones are more expensive to produce and travel at higher speeds. Despite their lower relative frequency in the simulation, they pose a greater risk to defended assets with a hit probability of 90% upon reaching the asset.

3.2 Defence System Components

The project focuses on ground-based defensive equipment that are either mounted on the defended ground assets or deployed as stationary systems. As discussed in section 2.2, the defence is simplified as consisting of detection and neutralization (interception). Thus, the defence system in the simulation is composed of two main categories: detectors, which detect UAVs prior to engagement, and effectors, which engage and neutralize threats once detected. The selection and configuration of these systems are instrumental in determining both the cost-efficiency and tactical effectiveness of the C-UAV solution.

Detectors represent various sensor types with differing capabilities in terms of range, effectiveness, and cost. The complete list of implemented detection systems is in Table 2. The performance of each detector is influenced by both the type of threat being detected and the distance between the threat and the detector. Detectors differ in operational range and effectiveness, with advanced systems such as active radars providing long-range coverage, while lower-cost alternatives offer economically efficient but more limited detection.

Effectors are the active countermeasures deployed to neutralize or destroy threats once they have been detected. These include kinetic systems, such as remote weapon stations, as well as non-kinetic technologies like radio frequency based interference and GPS jamming. Table 1 shows the listing of the selected effectors. Similar to detectors, each effector varies in range, effectiveness and cost. Kinetic systems generally offer high reliability at short distances, while electronic countermeasures can cover a broader area at potentially lower cost per engagement.

Both types of countermeasures are modeled using distance-dependent probability functions that reflect their performance. The mathematical formulation of these probability functions, including their parametrization and behaviour under varying environmental conditions is presented in the next section.

3.3 Probabilistic Modeling

In the simulation model for the C-UAV system, both detection and neutralization of UAV threats are probabilistic events. These probabilities are modeled as continuous functions of distance between the threat and the defending asset. Specifically, parabolic functions are used to define the value of p, which is the probability parameter in binomial trials that determines whether a detection or a neutralization of a threat occurs.

The polynomials used to approximate the probabilities are given as

$$p(x) = ax^2 + bx + c, \tag{1}$$

where $p(x) \in [0, 1]$ is the probability of detection or interception at distance x and a, b and c are parameters fitted to performance data on each type of detector and effector.

The parameters a, b and c of each polynomial were estimated by interpolating from Patria personnel's assessments corresponding to the 10%, 50% and 90% effectiveness levels at distances x_{10}, x_{50}, x_{90}, respectively. A system of equations is solved to fit the quadratic curve through the three points.

$$\begin{cases} p(x_{10}) = 0.1 \\ p(x_{50}) = 0.5 \\ p_(x_{90}) = 0.9 \end{cases} \Rightarrow \begin{cases} ax_{10}^2 + bx_{10} + c = 0.1 \\ ax_{50}^2 + bx_{50} + c = 0.5 \\ ax_{90}^2 + bx_{90} + c = 0.9 \end{cases} \tag{2}$$

The probability functions are visualized in figures 1–4. Short-range and long-range systems are plotted separately to improve visual clarity, with the distinction made based on their maximum effective distance. Each curve describes the success probability $p(x)$ of either detecting or neutralizing a UAV at distance x. The black horizontal line represents the constant probability value of $p(x) = 0$, showing that beyond the maximum effective distance of each countermeasure has no further capability to detect or neutralize the threat. In the plots, solid lines represent effectors, while dashed lines represent detectors.

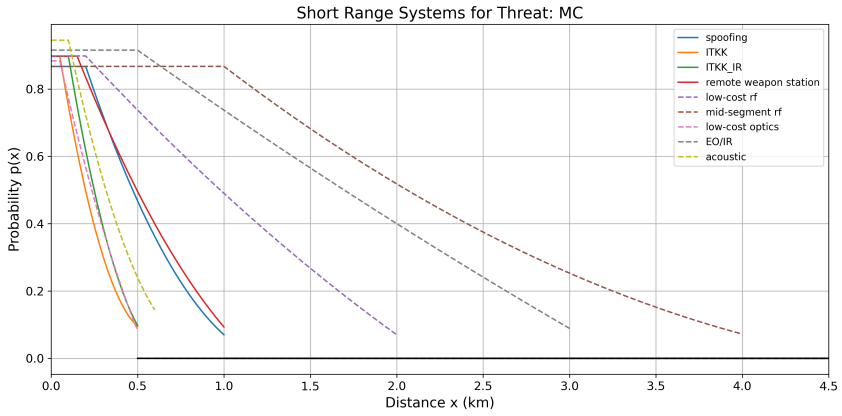

Figure 1: Probability functions for short-range countermeasures against multicopter (MC) threats.

When multiple detectors or effectors operate simultaneously, their combined effectiveness is modeled using the complement rule for independent events:

$$P_{\text{combined}}(x) = 1 - \prod_{i=1}^{n} [1 - p_i(x)]. \tag{3}$$

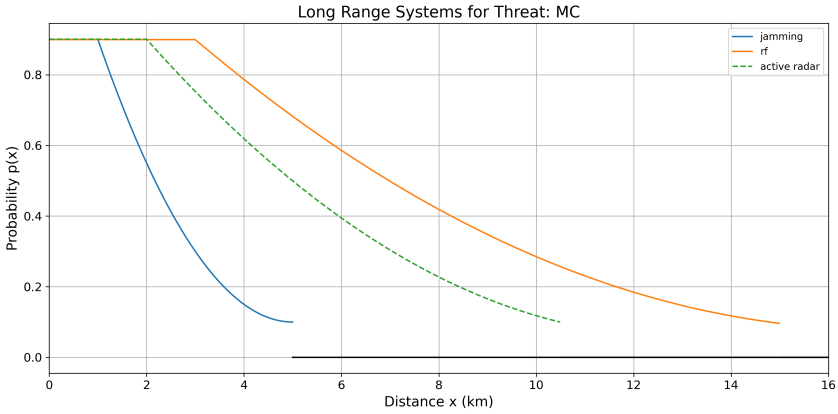

Figure 2: Probability functions for long-range countermeasures against multicopter (MC) threats.

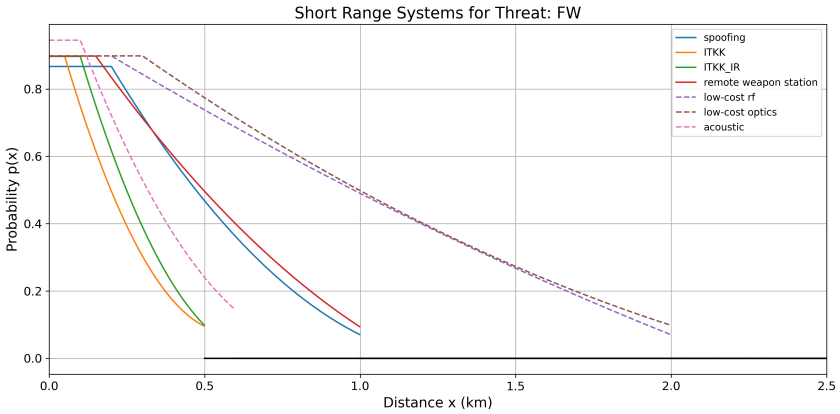

Figure 3: Probability functions for short-range countermeasures against fixed-wing (FW) threats.

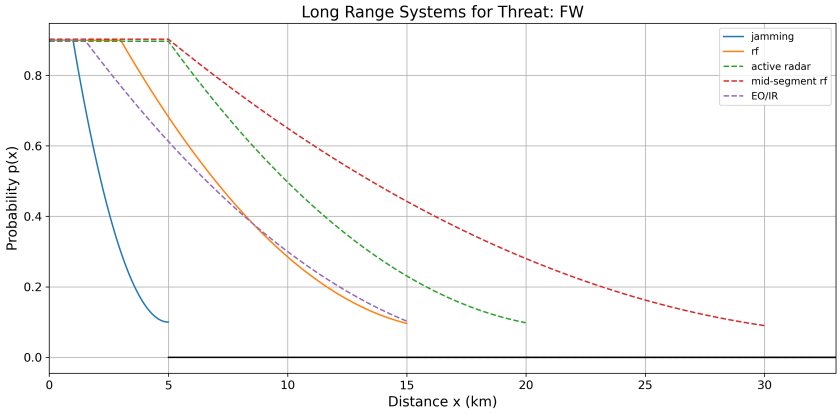

Figure 4: Probability functions for long-range countermeasures against fixed-wing (FW) threats.

3.3.1 Environmental Effects on Detection and Interception

Environmental conditions affect the performance of both detection and neutralization systems. Factors, such as fog and lightning conditions, can reduce the effectiveness of sensor-based systems.

To account for adverse weather conditions or terrain effects, the probability function is adjusted by an environmental visibility factor $k \in [0, 1]$ such that

$$p_{mod} = k \cdot p(x), \tag{4}$$

where $k = 1$ for clear conditions and decreases with reduced visibility.

The multiplicative adjustment ensures that the impact of environmental factors is reflected consistently accross different engagement ranges.

4 Simulation

The object of this study is to find cost effective defence measures against unmanned aerial systems. To answer the question, a simulation based approach was used to look at how different defence configurations can, on average, perform against attacks of UAVs. The cost effectiveness can be measured using the cost of the defence configuration, average cost of lost assets in a single attack, standard deviation of these costs in a single attack and the average number of lost assets in a single attack.

4.1 Implementation

The simulations were implemented in Python 3.12 using relevant scientific libraries, such as Numpy and Matplotlib. The structure of the simulations follows a basic OOP paradigm. A more detailed description of the class structure is provided in the UML diagram in Figure 5. The class Observer in the figure correspond to the detectors discussed in this report. The code repository is in appendix A.1.

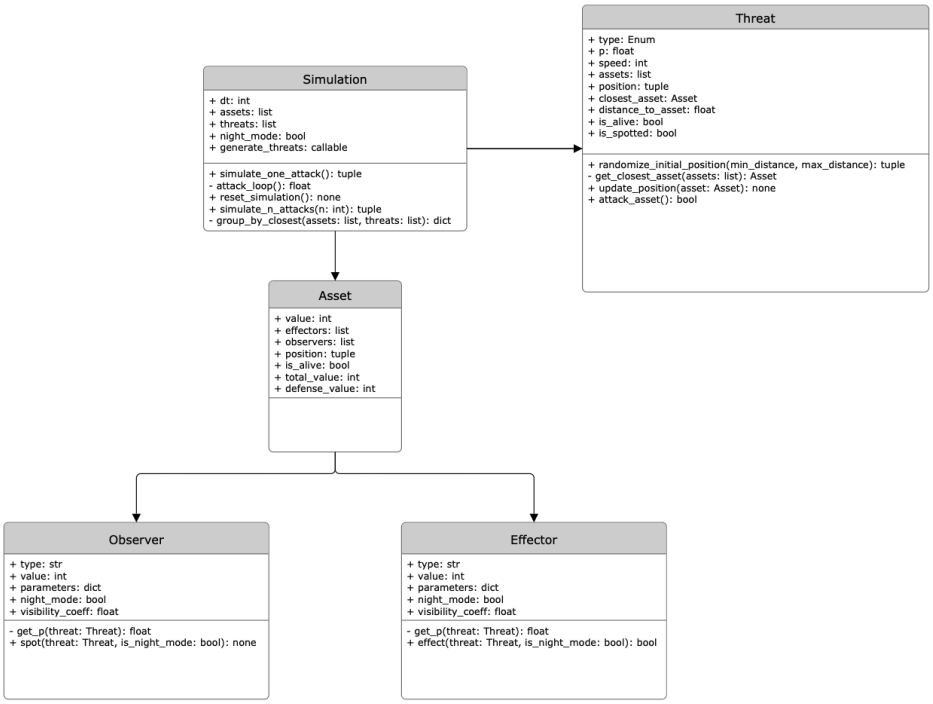

Figure 5: Class structure of the implemented simulation.

Each simulation is parameterized by a visibility coefficient k and a Boolean value indicating whether it is day or nighttime, since some of the defence measures are effective only during day time. In the simulation, assets are positioned on a 2D grid and each asset on the grid is initialized with a set of defence measures i.e. effectors and detectors. An exhaustive list of both effectors and detectors used in the study along with their parameters is in Tables 1 and 2. Both drone types, multicopters and fixed-wing drones, are parameterized by λ, which denotes the expected number of a given drone type in a single attack. The total number of each drone in a single attack is then sampled from a Poisson distribution at the start of each simulation. Initially each drone is placed randomly around the defence configuration by sampling a position from a ring with a minimum distance x_{min} to the defence configuration and a maximum distance x_{max}.

Table 1: Effectors and their parameters in the simulations.

Effector	**Cost**	**Effectiveness (distance)** 10% / 50% / 90%		**Parameters** $p = ax^2 + bx + c$
		Multi copter	**Fixed-wing**	
GPS jamming	6k €	5/2/1 km	weak	$a = 0.05,\ b = -0.5,\ c = 1.35$
GPS signal spoofing *	20k €	1/0.5/0.2 km (± 100 m)		$a = 0.67,\ b = -1.8,\ c = 1.2$
Radio-frequency jamming *	30k €	15/7/3 km		$a = 4.17 \times 10^{-3},\ b = -0.142,\ c = 1.288$
12.7mm air defence gun	5k €	0.5/0.2/0.05 km		$a = 2.96,\ b = -3.41,\ c = 1.06$ **Note:** $x \gg 0.5$ does not work
With IR sight option	20k €	0.5/0.3/0.1 km		$a = 2.67,\ b = -3.6,\ c = 1.23$ **Note:** $x \gg 0.5$ does not work
Remote Weapon Station (12.7 mm)	200k €	1/0.5/0.15 km		$a = 0.403,\ b = -1.41,\ c = 1.10$
Notes	* Usually come in the same package			

Table 2: Observers and their parameters in the simulations.

Observer	**Cost**	**Effectiveness (distance)** 10% / 50% / 90%		**Parameters** $p = ax^2 + bx + c$
		Multicopter	**Fixed-wing**	
Active Radar	1MM €	10.5/5/2 km	20/10/5 km	$a = 7.18 \times 10^{-3},\ b = -0.184,\ c = 1.24$ $a = 2.67 \times 10^{-3},\ b = -0.12,\ c = 1.43$
Passive RF				
Low-cost	1k €	2//0.2 km		$a = 0.05,\ b = -0.57,\ c = 1.01$
Mid-segment	200k €	4/3/1 km	30/10/5 km	$a = 0.042,\ b = -0.475,\ c = 1.3$ $a = 9 \times 10^{-4},\ b = -0.064,\ c = 1.2$
	5k €	0.5/0.3/0.05 km	2/1/0.3 km	$a = 1.11,\ b = -2.39,\ c = 1.0$ $a = 0.101,\ b = -0.703,\ c = 1.1$
EO/IR	80k €	3/2/0.5 km	15/10/1.5 km	$a = 0.013,\ b = -0.376,\ c = 1.1$ $a = 0.0023,\ b = -0.097,\ c = 1.04$
Acoustic	1 k €	0.6/0.4/0.1 km		$a = 1.58,\ b = -2.71,\ c = 1.2$

Once the assets and drones have been initialized, time advances in discrete steps dt. During each time step the drones move towards the closest asset and the defence measures aim to detect and neutralize the threats by sampling from a binomial distribution where p is parameterized by the assets distance to the threat. Once a drone is detected, the information is shared between all assets and every effector in the configuration can attempt to neutralize the drone. One effector can only destroy one threat during a time step dt. If a threat makes it to the asset, it will try to destroy it by sampling from a binomial distribution where p is a fixed probability distinct for both drone types. If the sampled attack is unsuccessful, the drone is considered to have missed and is destroyed. The simulation ends when either all assets or all threats are destroyed. The simulation is repeated n times for all defence configurations to gain an understanding of the average defence ability of the configuration.

It is obvious that this kind of simulation is too simple to capture all the intricacies of a real life defence scenario, but it provides a sandbox environment for comparing different arrangements. Moreover, the parameterization of the threats, effectors and detectors has a large impact on the simulation results and the results should thus be interpreted with due caution.

4.2 Configurations and Scenarios

To compare cost effectiveness, five different defence configurations shown in Figures 6 to 10 were developed. The configurations are based on materials provided by Patria. For each configuration, there are three sets of simulation parameters or scenarios described below. The setting is the same for all configurations, in the center there is a headquarter and a mortar team. On the side of the roads there are in total four groups of three Patria Pasi armoured personnel carriers (APC) and one group of logistics vehicles. The HQ is given a value of 1M € and each other points are valued at 500k €. These values are arbitrary, and are only used for comparison of defence arrangements.

Scenario 1: Perfect visibility ($k = 1$) and daytime.

Scenario 2: Perfect visibility ($k = 1$) and nighttime.

Scenario 3: Low visibility ($k = 0.5$) and daytime.

Figure 6 shows the most expensive defence configuration. In this configuration each asset has at least one defence measure and most have multiple.

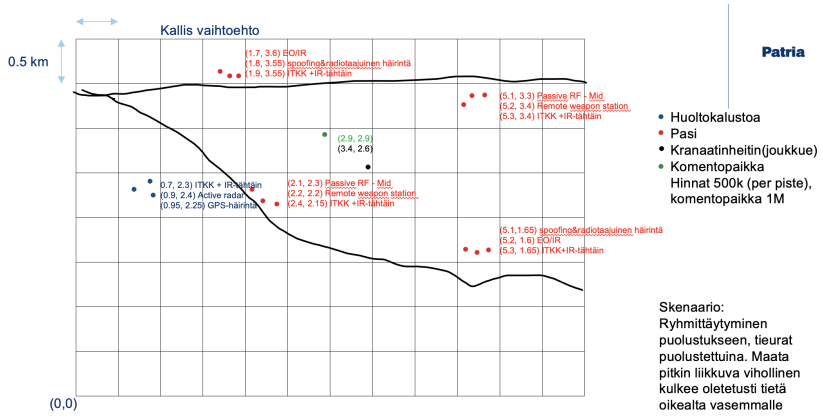

Figure 6: Configuration 1

Configuration 2 in Figure 7 is the second most expensive configuration. Two of the APC groups have GPS jammers, EO/IR sensors and 12.7mm air defence guns. The other two APC groups have EO/IR sensors and 12.7mm air defence guns with night vision sights for nighttime capabilities. The logistics group has one GPS jammer.

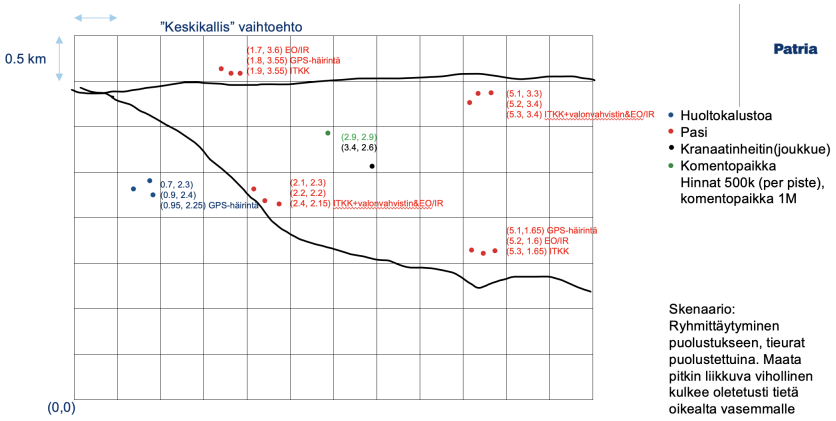

Figure 7: Configuration 2

Configuration 3 in Figure 8 is the middle one in terms of value of defence arrangements. Here each group of APCs has 12.7mm air defence gun with one passive radio frequency sensor and GPS jammer. The logistics units are equipped with a GPS jammer and a passive radio frequency sensor.

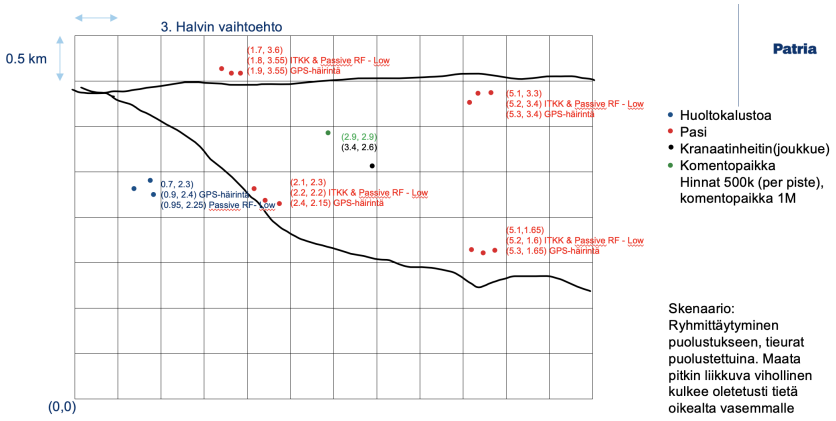

Figure 8: Configuration 3

in Figure 9 is the second least costly defence configuration. In this configuration each group of APCs and the logistics group are equipped a GPS jammer and a passive radio frequency sensor.

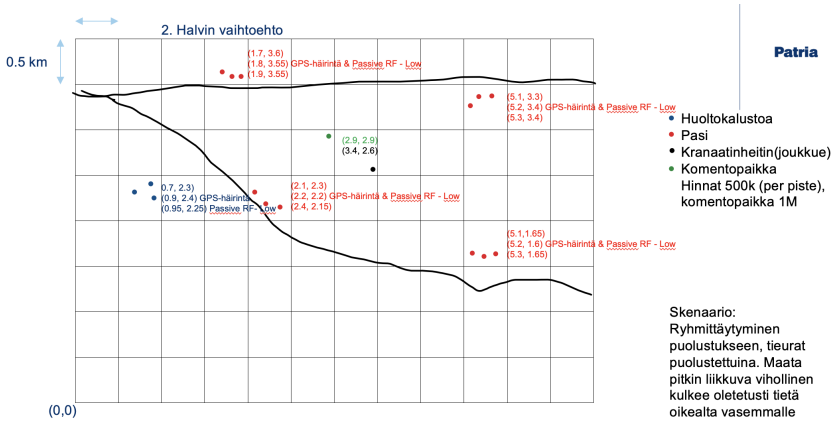

Figure 9: Configuration 4

In Figure 10 is the least costly defence configuration. In this configuration each group of APCs has 12.7mm air defence gun and one passive radio frequency sensor. The logistics units are equipped with a GPS jammer and a passive radio frequency sensor.

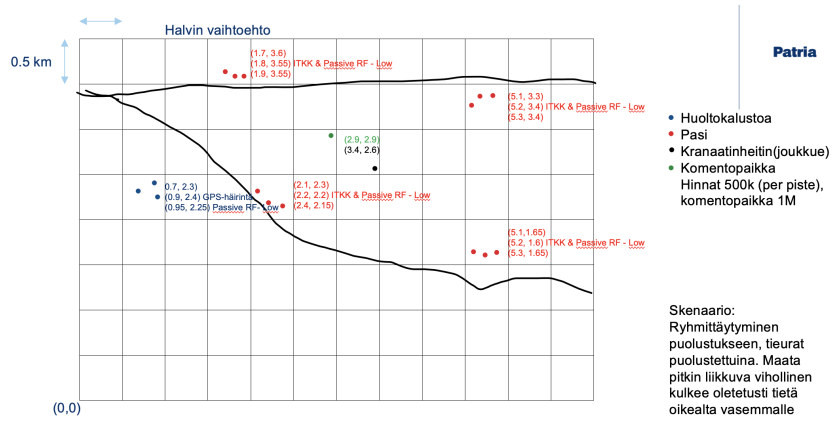

Figure 10: Configuration 5

5 Results

The results of the simulations done on the configurations from section 4.2 are presented in table 3.

Table 3: Simulation results for each configuration and parameter set.

Configuration	Scenario	Defence (€)	Damage (€)	Std. of Costs (€)	Lost Assets
1	1	2 166 000	2 063 782	1 189 864	3.28
	2	2 166 000	2 074 648	1 211 640	3.31
	3	2 166 000	2 075 926	1 193 636	3.31
2	1	388 000	1 715 139	912 272	3.22
	2	388 000	1 722 428	909 972	3.24
	3	388 000	1 723 925	932 897	3.24
3	1	55 000	1 273 905	708 982	2.51
	2	55 000	1 690 838	910 728	3.32
	3	55 000	1 291 061	725 982	2.54
4	1	35 000	1 251 455	694 183	2.47
	2	35 000	1 251 305	698 033	2.47
	3	35 000	1 259 442	696 974	2.49
5	1	31 000	1 266 947	710 934	2.50
	2	31 000	1 699 792	920 905	3.35
	3	31 000	1 287 776	716 433	2.54

Defence indicates the value of defence equipment (detectors and effectors) within a certain configuration, damage is the average value of assets and defence equipment lost and lost assets is the average number of assets destroyed within the simulations.

According to the results, increasing the defence measures seems to have weak positive correlation with the amount of costs and losses, and the variance of costs. The smaller amount of defence measures gives a better outcome for the average losses. In general, the nighttime and lower visibility do on average cause more losses than the perfect conditions. Nighttime seems to cause more issues than other visibility issues for the configurations' performance.

Configuration 4 seems to perform the best out of all the configurations as it clearly has the lowest cost while being consistent within the different conditions. Configurations 3 and 5 also perform relatively cost-efficiently in perfect conditions and low-visibility conditions. However, they struggle a lot more in nighttime conditions which would make them a less viable option altogether due to the higher amount of lost assets. Both configurations 1 and 2 are relatively consistent between the scenarios but clearly worse than the other configurations with the higher costs and higher number of lost assets.

6 Discussion

While the simulations have a baseline that works and the procedure gives some results, it is clear that the results do not intuitively make sense. This implies there likely exists some unknown issue within the simulation or parametrization that has not been identified at this time. The amount of lost assets should decrease with increased defence equipment as there would be more opportunities to detect and eliminate the aerial threats on average.

There might be a bug in the simulations such that the detecting asset does not communicate the detected threat effectively. For example, in configuration 4 the GPS jammers are on the same asset as the detectors, while in configuration 5 the jammers are on different assets than the detectors. Configuration 4 is notably better than configuration 5 in the nighttime scenario, where the GPS jammers are the only working effectors. This failure in communication would also explain the difference between the effectiveness of configuration 1 and configuration 5. The groups have significantly better defence equipment in configuration 1. However, configuration 5 has the detectors and effectors on the same asset in the APC groups, while the detectors are always on an asset without effector in configuration 1.

A notable amount of difference between the configurations in the costs of losses and the variance in costs may arise from losing the defensive equipment placed on the assets.

Comparing the different effectors with Figures 1–4, it seems clear that GPS jamming is a very good option for neutralizing threats. Thus, it is quite reasonable that the configuration 4 worked well. Combining with the analysis above, it would be interesting to give some asset the only effector even more effective than GPS jamming, radio-frequency jamming with some detector and see, if the model would work even better with them.

6.1 Heuristic approaches

The simulation script is able to produce some results and would likely be useful when the specific errors are fixed. However, due to the scale and difficulty of the whole problem, finding optimal solutions through, for example, brute force approaches is not computationally reasonable for long-term usage. Some good simulation solutions for specific situations could be done within a reasonable amount of time but adding further scenarios and attempting to generate the best possible solution in general is extremely hard without prior knowledge. Thus most of the configurations should be done heuristically as reducing the search space and the amount of scenarios that need to be considered is a lot better. With the ever changing field of warfare it is likely beneficial to be able find heuristically good enough solutions

The model itself is built with possible new additions of drone types, drone behavior and defence equipment in mind. Additionally, the current attributes of the equipment and drones are easily changeable if the attributes or features. Effective analysis of the actual cost-effective solutions and finding strategies which are viable in an actual battle setting would require further expert knowledge and applications of drone attack patterns and other strategies.

6.2 Sensitivity analysis

Conducting sensitivity analysis on the parameters of detectors and effectors was discussed, but could not be fitted into the schedule of the project work. The probability functions were modeled as parabolic functions, since one of the possible assumptions for the model was that probability of detecting and neutralizing would be inversely proportional to the square of the distance. Parabolic functions were chosen, since they decrease faster (when implemented correctly) than just simple linear functions and the probabilities were interpolated from three different points.

Some discussion was had to conduct sensitivity analysis using strictly inversely proportional (to the second power) probability functions of form $p = d \cdot 1/x^2 + e$. These functions would be interpolated from the points x_{10} and x_{90}.

Since the numbers x_{10}, x_{50} and x_{90} were the estimations of professionals at Patria, this kind of sensitivity analysis could be the first thing considered after getting the simulation to run perfectly as intended.

7 Conclusions

This project had the aim to create the sufficient tools to consider cost-efficiency between options for defence when the primary considered threats are unmanned aerial systems, or drones. The field of study on this project was unfamiliar to the team. However, applicable literature on the topic was found and workable simplifications and modeling was conducted on grounds of this literature.

A company sized troop was considered to be the main goal of defence and this was divided into different assets. Defence was split in two parts, detecting and neutralizing threats, with multiple possible equipment for managing both parts. The effectiveness of the equipment was modeled as decreasing with the distance to the drone increasing. The threats were placed into two categories, multicopters and small fixed-wing drones.

To simulate uncertainty and machinery errors within real life, the simulations were chosen to follow Bernoulli trials with changing probabilities which should by physical consideration have dependency on the square of distances. Thus the success probabilities were modeled with parabolic polynomials and fitted between certain estimates made by professionals at Patria.

The simulations were done with Monte Carlo methods where a large number of simulations are done to find average losses on specific troop configuration with different types of defence equipment under randomly generated attacks by unmanned aerial systems. From the simulations mainly the average cost of asset losses and the cost of losses are saved and considered for the analysis of the results. In general the problem became hard to fully analyze with the added scenarios and a large amount of defendable assets and thus a notable amount heuristic considerations of reasonable configurations and defensive equipment placements were made to reduce the amount of simulations that need to be ran. Further sensitivity analysis on the fitting parameters and other equipment would be a good point of research.

Overall results somewhat counterintuitively indicate that configurations with large amounts of defensive equipment lead to results where more damage to assets is observed than in configurations with less defensive equipment. This is likely due to a bug within the code causing such behaviour as such results do not make sense within the context of the simulation. From the low cost configurations it is found that GPS jamming is a cost-effective defensive option consistently within in different scenarios studied. For further studies the bugs within the script should be first fixed and the configurations should be recalculated and reconsidered. From there proper analysis could be made.

References

Juan A Besada, Ivan Campaña, David Carramiñana, Luca Bergesio, and Gonzalo de Miguel. Review and simulation of counter-UAS sensors for unmanned traffic management. *Sensors*, 22(1):189, 2021.

Konrad D Brewczyński, Marek Życzkowski, Krzysztof Cichulski, Kamil A Kamiński, Paraskevi Petsioti, and Geert De Cubber. Methods for assessing the effectiveness of modern counter unmanned aircraft systems. *Remote Sensing*, 16(19):3714, 2024.

Scott H Brooks, Carol Jacobus, Camron G Kohestani, John A Stikar, and Erik J Faye. Counter unmanned aircraft systems market survey (UUR). Technical report, Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), 2019.

Dharmendra Chauhan, Harshil Kagathara, Hiren Mewada, Sagar Patel, Sagar Kavaiya, and Gordana Barb. Nation's defense: A comprehensive review of anti-drone systems and strategies. *IEEE Access*, pages 1–1, 2025.

Cheng Fangzi, Zheng Wenrui, and Xu Chengjun. Research on modeling method of close-range anti-uav swarm combat simulation. In *2024 IEEE 2nd International Conference on Sensors, Electronics and Computer Engineering (ICSECE)*, pages 1044–1048, 2024.

Honggu Kang, Jingon Joung, Jinyoung Kim, Joonhyuk Kang, and Yong Soo Cho. Protect your sky: A survey of counter unmanned aerial vehicle systems. *IEEE Access*, 8:168671–168710, 2020.

Gökhan Karadeniz, Ahmet Özcan, Mehmet Bayram, and Gökhan İnce. Drone wars 3d: A game-based simulation platform for testing aerial defence strategies against drone swarms. *Journal of Aeronautics and Space Technologies*, 17(Special Issue):182–207, 2024.

Rajanikanth Nagaraj Kashi, Anushka Prashanth, Sumukh Rajanikanth Kashi, and Gayathri Prabhakara. A survey and analysis of drone detection systems using a systems approach superposed on scenarios. *Systems Engineering*, 27(3):598–636, 2024.

Seongjoon Park, Hyeong Tae Kim, Sangmin Lee, Hyeontae Joo, and Hwangnam Kim. Survey on anti-drone systems: Components, designs, and challenges. *IEEE Access*, 9:42635–42659, 2021.

Juho Roponen, David Ríos Insua, and Ahti Salo. Adversarial risk analysis under partial information. *European Journal of Operational Research*, 287(1):306–316, 2020. ISSN 0377-2217.

Choon Seng Tan, Douglas L Van Bossuyt, and Britta Hale. System analysis of counter-unmanned aerial systems kill chain in an operational environment. *Systems*, 9(4):79, 2021.

A Appendix

A.1 Project Github

Project Github can be found from `https://github.com/ahtikorhonen/case-studies-in-or`.

B Self Assessment

How closely did the actual implementation of the project follow the initial project plan? Were there any major departures and, if so, what?

The actual implementation of the project followed the initial project plan closely in terms of structure and, in the beginning, timeline. The major stages of literature review, data structuring, model design, simulation implementation and analysis were completed in the intended order. However, the implementation of the timeline towards the end of the project did get stretched, with some simulations run in the beginning of May. This was mostly due to the fact that different team members built on results of other members, and with a tight schedules outside of the project, the waiting times for results from other members were hard to predict, causing some difficulties in scheduling.

Some changes involved the modeling architecture. Night-time mode handling or visibility coefficients were not specified in the project plan. These were introduced during development to make simulations more reflective of real-world variability in sensor and effector performance.

In what regard was the project successful?

The first task of the project was to configure an appropriate framing of the problem. This was a very important and difficult task, since the initial problem formulation was very open. The framing was successful, providing meaningful goals and steps towards them.

A functional and modular simulation model capable of modeling UAV threats and evaluating the effectiveness of various countermeasure configurations was developed by the team.

The probabilistic modeling of detection and interception using parabolic distance-based functions turned out to be an effective abstraction and the simulation results behaved plausibly.

Additionally, the team collaborated dynamically throughout the project. Communication with the client was consistent and task distribution was generally well balanced.

In what regard was it less so?

One shortcoming was the limited validation of model parameters, especially for the sensor effectiveness in adverse environmental conditions. While reasonable assumptions were used, more thorough empirical grounding, such as test data or expert-reviewed parameter ranges, would have strengthened the credibility of the model. Greater integration of feedback from Patria during model calibration could have improved the realism of the outcomes.

The simulation model, while working and producing somewhat reasonable results did not work exactly as planned, that is, the results do not seem compatible with our assumptions. There might be some problems with the implementation, one hypothesis is that the assets do not share the information of detection efficiently.

What could have been done better, in hindsight? (you may analyze this question from the roles of the project team, the client, and the teacher(s))

With more time, more configurations could have been compiled using the results of initial configurations. This way the results could have been clearer and some debugging could have been done for the simulation.

More and earlier discussion on the key figures for evaluating cost effectiveness could have resulted in more concise key figures and more intuitive comparisons between the configurations.

The accuracy of parameters provided by Patria could have been better justified. However, it is understandable that would this information exist, it could be too sensitive to publish for the project team.