Development of a Concept of Operations for a Counter-Swarm Scenario

Jari Laarni[1], Antti Väätänen[1], Hannu Karvonen[1], Toni Lastusilta[1] and Fabrice Saffre[1]

[1] VTT Technical Research Centre of Finland Ltd, Espoo, Finland

Abstract. This paper describes a Concept of Operations (ConOps) for a counter-swarm scenario in which the defender side uses a swarm of drones to defend a target against an attacking drone swarm. A ConOps is a high-level conceptual description of how the elements of a system and entities in its environment interact in order to achieve their stated goals. It has shown to be a useful and integrative element in designing complex technical systems. The ConOps for a counter-swarm scenario presented in this paper will provide answers, among others, to the following questions: how the two drone swarms are deployed, how a scenario is introduced to the simulation system, and how its progress is monitored and supervised. A preliminary version of the ConOps for a counter-swarm scenario was drafted through by using a counter-swarm simulator and conducting discussions and interviews with military experts of the Finnish Defence Forces.

Keywords: Robotic swarm, Counter-swarming, Concept of operations.

1 Introduction

Highly autonomous and intelligent swarms of robotic vehicles are becoming more popular in the military domain, since swarm systems can perform many kinds of tasks more effectively and efficiently than a single device. Swarm robotics is a technical approach aiming to develop multi-robot systems, which are based on many cost-effective robots. Here, we present the development of a Concept of Operations (ConOps) for a counter-swarm scenario in which the defender side uses a swarm of drones to defend a target against an attacking drone swarm. A ConOps is a high-level conceptual description of how the elements of a system and entities in its environment interact in order to achieve their stated goals. It has shown to be a useful and integrative element in designing complex technical systems. The ConOps for a counter-swarm scenario will provide answers, among others, to the following questions: how the two swarms are deployed, how a scenario is introduced to the simulation system, and how its progress is monitored and supervised.

One key task in ConOps development is to define the main performance requirements for the system that is under development. We have conducted expert interviews, based on which we have drafted the key requirements for a swarm of robotic vehicles and counter-swarm actions, and compared them with the requirements identified in an earlier project. In this paper, we will also outline control concepts for a high-level control of a swarm of robots, including tasks such as situation assessment, coordination of task progress, alarm handling, and alerting other law enforcement units and manned vehicles to the situation.

The remainder of the paper is structured as follows: First, we review some relevant literature on counter-swarming. Second, we define the meaning of a ConOps on a conceptual level, give some examples of ConOps for robotic swarms, and present an earlier ConOps for a swarm of autonomous robotic vehicles in the military domain. Third, we present the summary of our interview results and the objective and progress of the development of a ConOps for counter-swarming scenario.

2 Relevant literature

First, we review some relevant literature on modelling and design of counter-swarming systems.

Several authors have reviewed possible ways of countering an attacking swarm of drones. According to [15], there are several methods of defending against an attacking swarm, which were classified into four groups, methods of destroying the attacker, collapsing, trapping and hijacking it. The first group is further divided into methods of shooting individual drones or their clusters with lasers, electromagnetic guns, or high-powered microwaves, or destroying an attacking swarm with another swarm. Kang et al. [9] published a detailed survey on counter unmanned vehicle systems in which they described some key counter UAV systems. First, they introduced several unmanned aerial vehicle (UAV) applications and regulations; second, they described various possible platforms, architectures, devices and functions of the counter UAV systems; and third, they reviewed the current features of the counter UAV markets.

Recently, Brust et al. [2] developed a swarm-based counter UAV defense system. The motivation for this study was that existing counter-unmanned aerial systems (C-UAS), which for the majority come from the military domain, lack scalability or induce collateral damages. Their system is based on an autonomous defense UAV swarm, capable of self-organizing its defense formation and to intercept a malicious UAV. The fully localized and GPS-free approach is based on modular design regarding the defense phases, and it uses a newly developed balanced clustering approach to realize intercept and capture formations. The authors also implemented a prototype UAV simulator. The resulting networked defense UAV swarm is claimed to be resilient to communication losses. Through extensive simulations, they demonstrated the feasibility and performance of their approach.

Strickland et al. [16] developed a responding system for unmanned aerial swarm saturation attacks with autonomous counter-swarms. The motivation to this study was that existing response systems are vulnerable to saturation attacks of large swarms of low-cost autonomous vehicles. One method of reducing this threat is the use of an intelligent counter swarm with tactics, navigation and planning capabilities for engaging the adversarial swarm. Both a Monte Carlo analysis in a simulation environment to measure the effectiveness of several autonomous tactics as well as an analysis of live flight experiments in swarm competitions were conducted in this study.

Several theses on counter-swarming have been written at Naval Postgraduate School in Monterey, California. Some of them have investigated the possibility to defend against attacking drone swarms by missile-based defense systems. Parsons'

[13] thesis explored the design of a counter-swarm indirect fire capability within the existing Marine Corps ground-based air defense and fire support framework. He developed a novel solution by defining the parameters of an artillery shell with effects designed to disrupt UAV operations. Such a shell would target the electromagnetic spectrum vulnerabilities of UAVs by utilizing expendable jammers delivered as a payload in a cargo-carrying projectile. This capability is likely to be effective against the swarm threat and can be used from the rear in support of units under UAV attack anywhere within range of the artillery piece. Thyberg [17] designed a low-cost delivery vehicle capable of deploying multiple guided munitions laterally out of the missile body at an altitude greater than that of the drone swarm. The guided munitions would be tasked by a targeting hub that would remain aloft above the specific drones, providing unique guidance commands to each deployed unit. This thesis focused specifically on the deployment of the munitions from a flight system, utilizing both Computational Fluid Dynamics and real flight testing to design an effective ejection mechanism and tracking approach. Additionally, high-level design and analysis of a targeting system within the missile was performed. The aim was to give the more cost-symmetric options and capabilities when it comes to air defense against drone swarms in the future. Lobo [11] designed sub-munition for a low-cost small UAV counter-swarm missile. The starting point was the possibility of defenses getting overwhelmed and the large cost asymmetry between currently available defenses and the cost of these threats. A survivability methodology was used to study the susceptibility and vulnerability of threat vehicles. The designed sub-munition possesses a low-cost affecting mechanism, such that multiple units could be delivered by a low-cost delivery vehicle. Experimental testing demonstrated the viability of the designs and the ability to provide a defense against small UAV swarms with low-cost technologies. Grohe [7] designed and developed a counter swarm air vehicle prototype. The motivation for this research was the fact that current air defense systems are designed to counter low quantities of very capable but extremely expensive weapons, and in many cases cannot properly defend against attacks involving a large number of offensive weapons. To avoid the scenario of an opponent overmatching current defenses with emerging low-cost weapons, a missile-based interceptor system was proposed. The chosen scenario was investigated using 'Repast Simphony' agent-based simulation. The aim was to deliver a payload capable of defeating multiple units, while still remaining cost-effective against the threat of low-cost small UAVs.

Several theses at Naval Postgraduate School in Monterey have studied swarm tactics with modelling and simulation tools. Gaerther [6] investigated UAV swarm tactics with agent-based simulation and Markov process analysis. Both defensive and enemy forces had the ability to launch a swarm of 50 UAVs, which are able to cooperate among their respective agents. The mission was to protect their own home base (i.e., the high value target) and to destroy the opposing one. Each side had the same type of UAVs with the same specifications. The scenario started with UAVs already launched. During the experiments, relevant factors, such as the initial positioning, spatial and temporal coordination, number of flights, and tactical behavior, were varied. Agent-based simulation and an associated analytical model were formulated. In agent-based simulation a UAV was modelled as an agent that follows a simple rule

set, which is responsible for the emergent swarm behavior relevant to defining swarm tactics. In addition, a two-level Markov process was developed to model the air-to-air engagements; the 1st level focused on one-on-one combat, and the 2nd level incorporated the results from the first and explores multi-UAV engagements. Diukman et al. [4] developed an integrative model to understand an opponent swarm. The integrative meta-model was based on an abstract description of the swarm objects (agents, C2 unit, and environment) and processes (transfer of EMMI (energy, material, material wealth, and information)). The Map Aware Non-Uniform Automata (MANA) agent-based simulation environment was used to explore different scenarios, such as Rally (attraction of swarm agents to one another in space), Avoid (swarm avoidance of a perceived threat object / entity), Integration (swarm agents capable of changing their local rule set in accordance to input stimuli), and Triangulation (locating the physical location of a LOS C2 unit based on observed swarm movement patterns). Day [3] studied multi-agent task negotiation among UAVs to defend against swarm attacks. Enemy agents sought to engage a high value defensive target. Defensive agents attempted to engage and eliminate enemy agents before they were able to reach the high value target. Baseline defensive strategy was a centralized solution to the optimal assignment problem. Centralized methods needed a centralized oracle that had near perfect situational awareness of the entire scenario at all times and near unlimited bandwidth to communicate with all of its assets. Distributed task assignment strategies were compared against the centralized baseline solution. They tried to remove above-mentioned constraints while striving to maintain solutions that approach optimal solutions otherwise found by centralized algorithms. In this study it was found that factors other than assignment method are more significant in terms of the effect on the percentage of enemies destroyed. These more significant factors were the number of defensive UAVs per enemies, the defensive probability of elimination and the speeds of defensive and enemy UAVs. Munoz [12] implemented an agent-based simulation and analysis of a defensive UAV swarm against an enemy UAV swarm. Enemy UAVs were programmed to engage a high value unit deployed in open waters, and a defensive UAV swarm aimed to counter the attack. The scenario was investigated using the above-mentioned open source simulation environment 'Repast Simphony'. Each defensive UAV launched has one enemy UAV assigned to it to engage. After its launch, the defensive UAV needs to predict the future position of the assigned enemy UAV. Then it needs to check the distance to the assigned enemy UAV. If the distance to the assigned enemy UAV is within the Blast Range, the defensive UAV blasts, and it has a probability of elimination associated with that explosion to determine if the assigned enemy UAV is eliminated or not. There were several controllable factors, such as enemy UAV speed, blast range, enemy UAV endurance, a critical number of enemy UAVs, detection range, and number of defensive UAVs launched per enemy. It was found that for defensive UAV to obtain a higher probability of elimination, the defensive UAV speed was recommended to be comparable, if not greater than, the enemy UAV attack speed. The number of direct hits the high value unit can withstand was significant.

According to the literature review, quite much theoretical research has been done about counter-swarming, but there are quite few real-life demonstrations – or at least public knowledge of them is limited.

3 Concept of Operations

The notion of Concept of Operations (ConOps) was introduced by Fairley and Thayer in the late nineties [5]. The first standard providing guidance on the desired format and contents of a ConOps document was IEEE standard 1362 [8]. Another relevance guide is the 2012 AIAA revision proposal Guide: Guide to the Preparation of Operational Concept Documents (ANSI/AIAA G-043A-2012) [1]. These documents define a ConOps as a description of a system's operational characteristics from the end user's viewpoint. The description can be considered as a boundary object aiming to communicate high-level quantitative and qualitative system information among the main stakeholders. ConOps documents can be presented in variety of ways due to the fact that they play different functions in different domains. Typically, ConOps documents are textual descriptions illustrated by images and informal graphics that portray the key features of the proposed system [16].

ConOps is considered as a knowledge artefact created during the early stages of the design process, but ConOps has potential to be used at all stages of the development process, and a high-level ConOps is a kind of template that can be modified and updated regarding specific needs and use cases [19].

A typical ConOps contains at a suitable level of detail the following kind of information [1]: possible existing systems and operations; proposed system operational overview, including items such as missions, operational policies and constraints, operational environment, personnel, and support concept and environment; system overview, including items such as system scope, goals and objectives, users and operators, system interfaces and boundaries, system states and modes, system capabilities and system architecture; operational processes; and analysis of the proposed system, including possible advantages and disadvantages, alternatives and trade-offs and regulatory impacts.

Typically, the ConOps development process includes at least three following main stages: First, background and motivation for the ConOps will be introduced, for example, by considering the operational task from an evolutionary perspective and by investigating how it has been developed throughout times. Second, the first version of the ConOps will be developed by identifying the preliminary needs, requirements and critical usage scenarios and outlining the first sketches of the system architecture, descriptions of user interaction with the system as well as conceptual illustrations and drawings. Third, all information is aggregated and synthesized as a final ConOps description specifying the main operational tasks and usage scenarios, and by this way laying the foundations for a well-grounded and shared understanding of the aimed future operation.

ConOps documents come in various forms, but at the system level, they typically describe the main system elements and their workings, stakeholders, tasks and functions, and goals and requirements.

3.1 Robotic swarm ConOps for the military domain

Previously, we developed a ConOps for a swarm of autonomous robotic vehicles in the military domain in MATINE funded project entitled "Development of a Concept of Operations for the operation of a swarm of robots" (RoboConOps) [10]. Our aim was to demonstrate how autonomic robotic swarms can be deployed in different military branches, that is, coast guarding at the littoral zone by the navy, air surveillance by the Air Forces and support for the urban troops operations. Each branch-specific ConOps contained the description of the mission goal, critical scenario description, main system requirements, system structure in the general level, and human-system interaction. The representative scenarios were brief fictional stories, which describe possible operative situations in the near future, when robotic swarms play an important role in military operations. Both normal and demanding operating situations were described in the scenarios. Performance requirements for the proposed system were based on expert interviews and workshops. A major part of the identified requirements focused on issues such as level of autonomy, data collection and tracing procedures, swarm navigation, human-robot interaction, operational robustness, weather-proofness and serviceability. Three system architectures were generated for each military branch, all of them consisting of elements such as robot nodes of the swarm, internal and external communication system, sensors and actuators, target, environment and control center. In the coast guarding scenario, underwater sensors and surveillance unmanned air vehicles (UAVs) monitor surroundings and if something abnormal is detected, send possible alarms and notifications to the swarm operation center. Cargo UAVs carrying unmanned under-water vehicles (UUVs) or surface vehicles (USVs) play an important role, for example, in reconnaissance missions. The operators are sitting in the command and control center and formulate and design the missions, supervise their execution and communicate with other stakeholders. The air surveillance system architecture is composed of various types of UAVs, such as cost-effective mini-UAVs, long-range surveillance UAVs and multifunctional UAVs. It is also possible to include manned aircrafts into the system architecture. In the Ground Force scenario urban troops are equipped with a fixed sensor and camera network, surveillance and cargo UAVs and multifunctional unmanned ground vehicles (UGVs).

Three control concepts for supervising the autonomous robotic swarms were developed for each military branch. The concepts describe operator roles in a detailed level and how these roles are connected to the technical systems and to other actors related to each military branch's operations. Air Force and Navy scenarios have two operators monitoring and supervising autonomous swarms with a workstation-based user-interface setup. In the Air Force scenario, one operator conducts mission planning, supervises its progress and reacts to possible exceptions in the control center. Another operator is in an intelligence officer role, making plans for missions together

with the other operator, building a common operational picture and analyzing and sharing gathered reconnaissance information. In the Navy scenario the command and control center is also manned with two operators. One of them monitors both the sensor network and the progress of the mission and manages alarms and unknown object information. Another one is responsible of special missions: he supervises robotic swarms during task execution and communicates awareness information for the land forces and manned vehicle units. In the Ground Force scenario one operator supervises the swarm in a workstation-based operation center, makes mission plans and monitors their progress. Another operator is working in the battleground and assigns detailed tasks such as building investigation and clearing missions to the swarm through a mobile user interface.

4 Objectives

4.1 Main aim and progress of work

In the present study our main aim was to develop simulations of swarm-based countermeasures to an attack conducted using a swarm of autonomous drones. For instance, we tested a defensive strategy by simulating autonomous UAVs ("scouts") with the ability to call upon a larger force when detecting a potential threat [14]. We anticipated that between ten and a hundred autonomous units (depending on the scenario) will be suitable to demonstrate the advantages of swarm-based defense. The project consisted of the following tasks: 1) implementation of a realistic 3D flight model with adjustable parameters; 2) testing robustness of the swarming behavior to errors and environmental conditions; 3) performance evaluation of the counter-swarm; 4) identification and simulation of typical scenarios; and 5) deployment cost evaluation.

Representative scenarios were selected based on discussions with military experts of the Finnish Defence Forces. The potential example scenarios include both military/law enforcement (e.g., radar station) and civilian targets (e.g., power plants). Emergent properties that result from the interplay between exogenous (e.g., the geometry and topology of the environment) and endogenous factors (e.g., the collective decision-making functions governing the behavior of the swarm) were thoroughly investigated and leveraged.

4.2 Methods

Six military experts were interviewed in 2021. The experts represented the Headquarters of the Defence Forces, the Headquarters of the Land Forces, the Naval Academy and The Finnish Defence Research Agency [14]. The interviews were held remotely through Microsoft Teams by two or three researchers. Interviews were audio-recorded provided that the interviewees consented to the audio recording. If the consent was not given, detailed notes were taken during the interview. Each of the interviews and group discussions lasted for two to three hours, and they were divided into two main

parts. First, there was a general discussion about the use of robotic swarms in military missions; and after that, there was a detailed discussion about the CounterSwarm simulator and the ways it could be further developed.

5 Results

5.1 Summary of interview results

Next, we present the main results of the expert interviews. This section is based on the MATINE summary report by Saffre et al. [14] The summary of the interviews presents opinions of individual experts, and thus does not reflect a consensus among all interviewees. In general, the interviewees thought that autonomous robotic swarms can be seen as a potential game changer of how the warfare is conducted. For example, the boundaries of military branches may become blurry, if all types of robotic swarms can be used in all military branches. Robotic swarms can be used on land, at sea and in the air, and swarming can also be applied in cyberspace. A war between drone swarms is technically possible in the near future, but poor weather and environmental conditions may compromise their effective use.

In general, ethical and judicial restrictions will prevent the use of swarms of autonomous vehicles in straight military offences [14]. The role of humans is to set limits to the warfare between autonomous systems and prevent further escalation of the situation. However, this becomes more difficult, as the tempo of warfare increases.

Encirclement and simultaneity are key features of military swarming: swarming makes possible to encircle the enemy drones and attack them simultaneously from multiple directions. A surrounding swarm can also conduct pulsing hit-and-run attacks by appearing and disappearing repeatedly. In order to achieve these positive impacts, a high level of autonomy is required so that the members of the swarm decide on how to act. Decision making is to a large extent decentralized and conducted where the operation is carried out.

Swarming promotes flexibility: the mission can be continued, even though a large part of the drones has been destroyed. Disposability and cost-effectiveness are key indicators: if the swarm is composed of inexpensive drones, the whole swarm can be sacrificed if needed. It is not necessarily feasible to incorporate both manned and unmanned units into swarms, because they may restrict each other's abilities. In principle, the collaboration between manned and unmanned systems is challenging, because a manned system quite easily slows down the progress of a mission.

In the first phase, autonomous swarms can be used in surveillance/reconnaissance operations and in area monitoring. For example, a drone swarm could conduct long-term patrolling in a military area, detect and recognize possible unknown objects and react quickly to them. Swarming provides new opportunities to decoy the enemy by saturating the airspace or leading new swarms periodically to the airspace. From the defender's perspective, it is very difficult to recognize armed drones carrying explosives or weapons from harmless units, if the airspace is saturated with these drones.

Since it is difficult to detect an attacking swarm of drones if it does not emit anything, a layered system is required for the detection and identification of the swarm. The layered system should be composed of various nonphysical systems (e.g., sensors, radars and lasers).

The defensive maneuvers against robotic swarms should include interfering and/or preventing communication. In principle, the best method to neutralize an attacking swarm of drones is to break the electronics of a drone with an electro-magnetic pulse. The drawback of this method is that it easily causes collateral damage, for example, destroys one's own devices at the same time. Physical mitigators such as projectiles and drones are especially suitable for counter-swarming. As discussed above, in our simulation another swarm counters an attacking drone swarm, and the drones of both swarms are equipped with weapons.

During the latter part of the interview, we carried out some simulator runs and discussed with the experts the key features of the simulation and the ways it could be improved (Fig. 1).

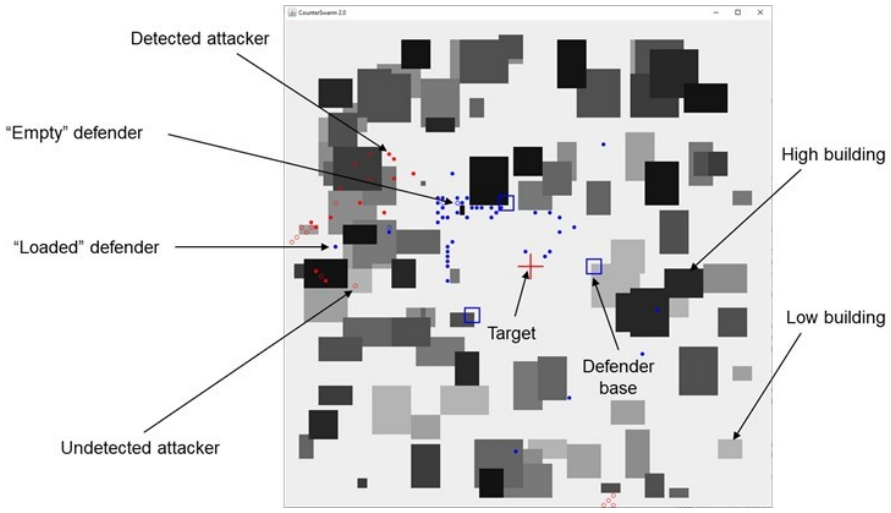

Figure 1: CounterSwarm simulator's situational picture with legends of the used symbols [14].

One of the interviewers presented the simulator to the interviewee. The interviewer noted that the simulator enables the investigation of complex behavior of autonomous drone swarms. For example, it is possible to test the influence of critical variables such as the relative size of attacking and defending swarms; and assault and guarding distance, as well as properties of individual units, like speed and resilience. Furthermore, the systematic analysis of the impact of control parameters enables the implementation of various tactics in the form of combinations of parameter values for the functions governing autonomous decision making by individual units, for example, pursuit, encirclement and perimeter defense. The effects of some of these parameters were demonstrated to the interviewee.

The interviewees thought that the simulator is useful in promoting tactical thinking about counter-swarming [19]. Several parameters were recognized as relevant for controlling the behavior of attacking and defending swarms such as assault and counter-attack distance and probability of change of direction. The interviewees also thought that it is important to continue to study the impacts of various control parameters on swarm behavior in counter-swarming context. Several improvements were suggested to the tactical control of robotic swarms such as division of a swarm into smaller groups, introduction of sub-tasks, optimization of a counter-attack and programming of new scenarios (e.g., reconnaissance).

5.2 Main elements of a ConOps for Counter-Swarming

Next we present the main characteristics of a ConOps for counter-swarming. The ConOps is based on information gathered through expert interviews and the results of simulations designed to study the performance of various attack and defence tactics.

Mission description. The main objective is to prevent a drone swarm to reach a predefined high-valued target by attacking against it. Special defender tactics for preventing the enemy drone to achieve its objective were developed. According to gathered intelligence, there is a danger of terrorists attacking strategic targets in big cities using drone swarms. The defender side has also intelligence knowledge of possible enemy tactics. The level of preparedness was raised based on the updated situational awareness.

Scenario definition. There is a big public event at a sports stadium. Terrorists make an attack by sending a drone swarm equipped with explosives towards the stadium. They have launched the swarm from a nearby air base, which has not been guarded. Provisions have been made for these kinds of attacks by identifying possible high-risk places (e.g., stadiums) and arming them with drone swarm stations or ordering moveable stations to the stadium for big public events.

Area surveillance is made by radars, and observations made about an approaching swarm triggers the operation of the defending swarm. Figure 2 illustrates the stadium defense scenario based ConOps diagram. The diagram visualizes and indicates the relationships between stakeholders, security control center with operators, and environment and air surveillance system with counter drone swarm units.

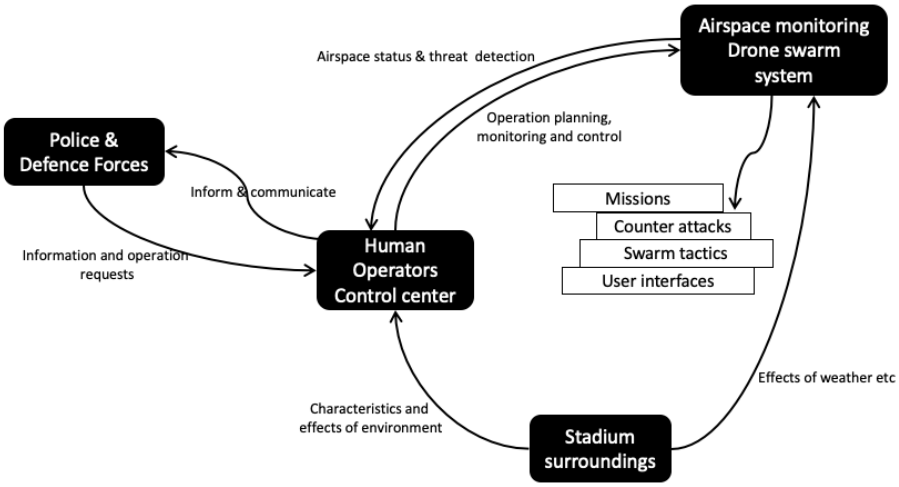

Figure 2: ConOps diagram of the sport stadium surveillance and defense scenario.

Main stakeholders. Public law authorities such as police take the main responsibility of organizing the swarm-based counter-swarm operation. Cooperation among authorities (e.g., with the defence forces) plays an important role. It is possible to purchase the counter-swarm service from private companies either partly or totally.

The station for a drone swarm with launch pads can be either moveable or immoveable. In the first case, it can be ordered by request to the place where the public event is held.

At the security control centre specialized operators plan, perform and manage the mission (intelligence operator, swarm operator etc.). Figure 3 shows the main tasks each of the operators are in charge of. An intelligence officer is responsible of mission planning and operation, a swarm operator is responsible of monitoring and control of the swarm, and a group of service personnel is responsible of the launch of the swarm and its return. In addition, operators at the control center have direct connection to the police headquarters, the defense forces and other authorities.

Operational environment. The dogfight occurs in the airspace above the target city. It is summer weekend, the weather is fair, and wind conditions favorable for drone operations.

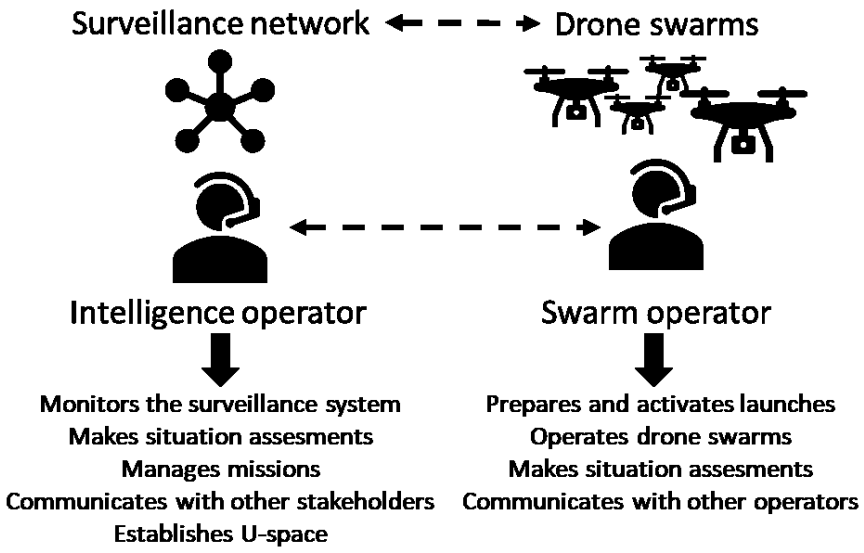

Figure 3: Security control center operators and their tasks.

Main phases of the scenario. One of the main elements of the ConOps is the description of the main phases of the mission. The mission can be divided into the following phases:

1) The system is switched to the state of full readiness, and preparations are made to the swarm mission.
2) Airspace is monitored by a radar system.
3) An approaching enemy swarm is detected, identified and classified.
4) A temporary restricted space around the stadium is set up to automatically secure the area of an air battle (so called U-space).
5) A method for countering the attacking swarm is selected (taken into account, e.g., the minimization of the risk of collateral damage).
6) An air-raid alarm is triggered.
7) The defender swarm is launched, and it is approaching the enemy swarm.
8) Primary tactics for swarm confrontation is selected.
9) The engagement between drone swarms starts.
10) Defender tactics is adjusted according to the enemy behavior.
11) The enemy mutually adjusts its tactics.
12) There is a culmination point of the air battle, after which the enemy swarm disengages the battle.
13) The defender swarm returns to the air base.
14) Maintenance and service operations are carried out.
15) Debriefing and reporting are completed.

Performance requirements. Some key success criteria are skilled application of swarm tactics (e.g., encirclement, simultaneity and pulsing attack) and ability to flexibly change defender tactics. Air dominance can be most easily achieved by the number of drones, i.e., by saturation of the airspace.

A repertoire of tactics are available providing the defender drone swarm the best possible chance of repelling the attack. Three tactical rules turned out to be successful in simulations: 1) quick response, in which the drone flies toward the attacker to intercept it some distance from the target; 2) limited recruitment capability in which defenders are allowed to respond to a threat detected by others, but only when they are already close to the event; and 3) restricted perimeter in which a retreating attacker is chased only a short distance away from the target, to avoid falling for decoy manoeuvres [14].

Persistence is important, since operations may last a quite long period of time in variable weather and lighting conditions. Resilience is also needed so that the swarm is able successfully complete its mission, even when several defender drones are destroyed. Level of autonomy can be changed during the mission, positioning cannot be only based on GPS, and communication between drones should be resistant to disturbances and failures.

Challenges and risks. Several challenges and risks have to be considered. For example, the risk of collateral damages is high in built environments; ethical and juridical challenges also have to be taken into account; and poor weather may compromise the defender tactics.

System interface (what is included in the system and what is not). The system consists of an autonomous swarm of flying robotic systems. Individual drones are compact, adaptable, reliable, durable, effective, capable of learning, and equipped with various kinds of payloads. A compromise between weight and feature set must be carefully made, however, a mix of different drones can facilitate the choice.

The system also includes a computer system with programming software for learning robots, communication system, user interface for communication between operators and robots, and carriers and launch pads

6 Discussion

In this research, a novel solution was developed against a hostile swarm of autonomous drones. Evaluation of the usefulness of the proposed counter-swarm approach helps to decide the applicability of the approach. For example, it can be determined in which scenarios (e.g., the protected area is of a specific size) it is viable to use the approach.

The ConOps approach makes it possible to understand and disclose motivations and possible barriers of usage activity among different user groups. The ConOps also helps to determine different modes for swarm management according to their com-

plexity. In the lowest level of complexity, one operator executes one mission by monitoring and controlling one specific robot swarm, and in the highest levels of complexity, multiple robotic swarms, operators and troops from different military branches operate in the same area and accomplish joint missions. Even though technological and human factors issues are seldom a critical bottleneck for the deployment of autonomous swarm robot systems, they are highly important from the end users' perspective, and they must also be adequately addressed in the ConOps. A fluent interaction between human operators and a swarm of robots means specific requirements for the operator and the system. The operator must be aware of the system and mission status, and user interfaces must be designed to present situation-aware information in a right manner. On the other hand, the system must adapt to different situations and react to operator actions.

Some of the main prospects of swarming were raised in discussions with military experts. Swarming can in general support traditional victorious warfare tactics and actions. Simultaneity and encirclement indicate that it is possible to center power around the enemy troops and attack them simultaneously from multiple directions; increased flexibility and resilience, in turn, indicate that there are more opportunities to change tactics on the fly, and it is possible to continue a mission, even though part of the swarm has been destroyed. It is also possible to saturate the area by covering the space with a swarm of cost-effective drones and to sacrifice the whole swarm in order to achieve some goal (i.e., disposability). These prospects have implications for how military missions will be executed in the future, and how the roles of human operators and military troops operating in the battlefield will change. For example, it is possible that the boundaries of military branches become more blurred with the increasing role of autonomous systems; there are new possibilities to decoy the adversary, and the rhythm and tempo of warfare may drastically increase. In order to achieve these prospects, global behavior of a swarm is more than a sum of the behavior of its parts. A swarm of drones should, among others, exhibit a high level of autonomy, distributed decision-making, and short-range communications. All these changes, in turn, have implications to human-swarm interaction. Human operator can be or should be out-of-the-loop, when the situation in the battlefield evolves very fast. On the other hand, ethical and legislative concerns should not be insurmountable, if one swarm of autonomous robots attacks another one.

The Concept of Operations for our counter-swarm scenario is divided into two main parts, detection, identification and monitoring of the adversary and attacking and defending. Regarding detection and identification, there are several challenges from the defender's point of view. It is difficult to track the approaching swarm, and identify it, if the attacking swarm approaches quietly. In a war of swarms, the most obvious way to destroy the adversaries is to shoot them down or crash against them, but it may have unwanted side effects that have to be considered.

Promising application areas for autonomous/semi-autonomous swarm of drones are, for example, intelligence, surveillance and decoy operations and guarding a military airbase or a service harbor. A swarm of UUVs patrolling under water can be used in anti-submarine warfare, and mine search and minesweeping. A war of swarms was considered to be realistic in the near future (i.e., within five to ten years).

7 Conclusions

The paper describes a ConOps for a counter-swarm scenario in which the defender side uses a swarm of drones to defend a target against an attacking drone swarm. A ConOps is a high-level conceptual description of how the elements of a system and entities in its environment interact in order to achieve their stated goals. It has shown to be a useful and integrative element in designing complex technical systems. The ConOps for a counter-swarm scenario will provide answer, among others, to the following questions: how the two swarms are deployed, how the scenario is introduced to the simulation system, and how its progress is monitored and supervised. A preliminary version of the ConOps for a counter-swarm scenario was drafted through a counter-swarm simulator and discussions with military experts of the Finnish Defence Forces.

8 Acknowledgements

This research was funded by the Scientific Advisory Board for Defence (MATINE) in the CounterSwarm project. In addition, the Academy of Finland is acknowledged for part of the financial support from the project 'Finnish UAV Ecosystem' (FUAVE, project grant number 337878).

References

1. American Institute of Aeronautics and Astronautics (AIAA): ANSI/AIAA guide for the preparation of operational concept document, G-043-1992, ANSI/AIAA G-043-1992, Reston, VA (1993).
2. Brust, M.R., Danoy, G., Stolfi, D.H., & Bouvry, P.: Swarm-based counter UAV defense system. Discover Internet of Things, 1(1), 1-19 (2016).
3. Day, M.: Multi-Agent Task Negotiation Among UAVs to Defend Against Swarm Attacks, Naval Postgraduate School, Monterey, California (2012).
4. Diukman, A. G.: Swarm Observations Implementing Integration Theory to Understand an Opponent Swarm, Naval Postgraduate School, Monterey, California (2012).
5. Fairley, R.E., Thayer, R.H.: The concept of operations: The bridge from operational requirements to technical specifications, Ann. Softw. Eng., vol. 3, pp. 417-432 (1997).
6. Gaerther, U.: UAV swarm tactics: an agent-based simulation and Markov process analysis, Naval Postgraduate School, Monterey, California (2013).
7. Grohe, K.: Design and Development of a Counter Swarm Prototype Air Vehicle. Naval Postgraduate School Monterey United States (2017).
8. IEEE: IEEE Guide for Information Technology - System Definition - Concept of Operations (CONOPS) Document, IEEE Std 1362™, IEEE CONOPS Standard. New York: IEEE (1998).
9. Kang, H., Joung, J., Kim, J., Kang, J., Cho, Y.S.: Protect Your Sky: A Survey of Counter Unmanned Aerial Vehicle Systems. IEEE Access, vol. 8, pp. 168671-168710 (2020).

10. Laarni, J., Koskinen, H., Väätänen, A.: Concept of Operations Development for Autonomous and Semi-Autonomous Swarm of Robotic Vehicles, in HRI '17 Companion, March 06-09, 2017, Vienna, Austria. ACM (2017).
11. Lobo, K.B.: Submunition design for a low-cost small UAS counter-swarm missile. Naval Postgraduate School Monterey United States (2018).
12. Munoz, M.F.: Agent-based simulation and analysis of a defensive UAV swarm against an enemy UAV swarm, Naval Postgraduate School, Monterey, California (2012).
13. Parsons, M.D.: Feasibility of indirect fire for countering swarms of small unmanned aerial systems. Doctoral dissertation, Monterey, CA; Naval Postgraduate School (2020).
14. Saffre, F., Karvonen, H., Laarni, J., Lastusilta, T., Väätänen, A.: CounterSwarm – Turning Collective Intelligence against Hostile Drone Swarms. MATINE summary report (2021).
15. Scharre P: Counter-swarm: a guide to defeating robotic swarms—war on the rocks (2017).
16. Strickland, L., Day, M. A., DeMarco, K., Squires, E., Pippin, C.: Responding to. In Ground/Air Multisensor Interoperability, Integration, and Networking for Persistent ISR IX (Vol. 10635, p. 106350Y). International Society for Optics and Photonics (2016).
17. Thyberg, R. I.: Design And Testing Of A Multi-Unit Payload Delivery And Tracking System For Guided Munitions To Combat UAV Swarm Threats. Naval Postgraduate School, Monterey, California, United States (2016).
18. Tommila, T., Laarni, J., Savioja, P.: Concept of operations (ConOps) in the design of nuclear power plant instrumentation & control systems. A working report of the SAREMAN project. VTT Working Report. Espoo: VTT (2013).
19. Väätäinen, A., Laarni, J., & Höyhtyä, M.: Development of a Concept of Operations for Autonomous Systems. In J. Chen (Ed.), Advances in Human Factors in Robots and Unmanned Systems (pp. 208-216). Springer. Advances in Intelligent Systems and Computing, Vol. 962 (2020).