SAFETY&DEFENSE
Scientific and Technical Journal ISSN 2450-551X

Factors Determining a Drone Swarm Employment in Military Operations

Tadeusz ZIELIŃSKI

War Studies University, Warsaw; t-zielinski@akademia.mil.pl,
ORCID: 0000-0003-0605-7684

DOI: https://doi.org/10.37105/sd.112

Abstract

The aim of this study is to identify a drone swarm's capabilities and the key factors influencing its employment in military operations. The research takes the quantitative analysis of scientific literature related to the technical and operational utilization of drones. The use of drones for military purposes in contemporary world is widespread. They conduct dull, dirty, dangerous and deep military operations replacing manned aviation in many areas. Progressive technological development including artificial intelligence and machine learning allows for the use of military drones in the form of a swarm. It is a quite new technology at the beginning of development. The study indicates that the capabilities of a drone swarm based on communication within the group and autonomy differentiate it from the typical use of unmanned aircraft. Size, diversity, self-configurability and self-perfection amongst the others indicated in literature are attributes of a drone swarm which may give advantage in military operation comparing to the classic use of unmanned aircraft. Emergent coordination as a command and control model of a drone swarm is a future way of utilizing that technology in military operations. In the future, a drone swarm will be a cheaper equivalent of advanced and much more expensive weapon systems conducting combat operations.

Keywords

autonomy, capabilities of drone swarm, command and control models, defense, drone swarm, military operations, unmanned aerial vehicle

Submited: 28.03.2021 Accepted: 30.04.2021 Published: 23.05.2021

1. Introduction

Progress in two critical technologies – artificial intelligence and machine autonomy – leads to the transformation of combat operations, in which the concept of a "drone swarm", consisting of cooperating autonomous robots that react over the battlefield as one organism, appears more and more often. Non-state actors have already demonstrated the effectiveness of mass attacks against conventional military and economic targets using drones. The first such an attack took place on the Russian air and naval bases in Hmeimim and Tartus in western Syria on the night of January 5/6, 2018. Thirteen GPS-guided drones participated in the attack. It was the first time that terrorists had organized a massive attack with unmanned aircraft sent over 50 km with the use of modern GPS satellite navigation system receivers. The application of this concept was further confirmed when around ten drones were used on September 14, 2019 to set fire to two Saudi Arabian "Aramco" oil processing plants in Abqarq and Khurais. The concept of a drone swarm was also applied in the recent conflict between Azerbaijan and Armenia in Nagorno-Karabakh. Leading military powers such as the United States, China, Russia and the United Kingdom are already involved in the development of this technology and have carried out numerous trials of drone swarm over the last 3–4 years. The United States has been conducting drone swarm tests since 2015. In January 2017, the US Strategic Capabilities Office and Air Force conducted trials with 103 Perdix Quadcopter Drones as swarm. The US Defense Advanced Research Projects Agency (DARPA) is also working on a program called "Gremlins," which includes microdrones with size and shape of missiles to be dropped from aircraft. Meanwhile, the US Navy is conducting an entire research program towards the development of autonomous swarms known as "Low Cost Unmanned Aerial Vehicle Swarm Technology" (LOCUST). Russia is also working on the concept of a drone swarm and is possibly trying to integrate drones into its "sixth generation fighters". The Chinese have also repeatedly demonstrated their capabilities and progress in this field.

The aim of the research is to identify drone swarm's capabilities and the key factors influencing its employment in military operations. The study allows the following research question to be answered: (1) what kind of capabilities describe a drone swarm? (2) what key factors determining the employment of a drone swarm in military operations? In order to answer these questions, a quantitative analysis of literature have been used. The first group of analyzed literature was related to the technological aspects of a drone swarm. Conclusions from the research allowed us to define a drone swarm and then identify and describe its capabilities and command and control models. The second group of literature was connected with the utilization of drones in military operations. By analogy, the scope of employment a drone swarm in military operations and dilemmas related to its autonomy have been identified.

2. Defining a drone swarm and describing its capabilities

SWARM stands for "Smart War-Fighting Array of Reconfigured Modules." John Arquilla and David Ronfeldt (2000, p. 8), authors of one of the first scientific studies on swarm technology in military applications, defined a swarm as "systematic pulsing of force and / or fire by dispersed, interneted units, so as to strike the adversary from all directions simultaneously". Paul Scharre (2014, p. 26), on the other hand, defines the swarm as "large numbers of dispersed individuals or small groups coordinating together and fighting as a coherent

whole". Robotics swarm can be thought of as a hybrid cooperative robotics that encompasses swarm and multiagent systems. It can consist of either homogenous or heterogeneous agents, which operate in different domains with varying system capabilities and complexity. Each agent is also capable of conducting a useful task, but at limited capabilities when compared to the entire swarm. The swarm's size varies but is large enough to cater redundancies to increase robustness. Its software also allows for scalability to increase the flexibility and dynamism (Tan & Zheng, 2013).

A drone swarm consists of multiple unmanned aerial platforms and / or weapon systems deployed to achieve a common goal. Air platforms and / or weapon systems autonomously change their behavior by communicating with each other. A drone swarm exhibit more complex behaviors than individual drones. This may include attack-capable platforms or existing weapon systems suitably modified to communicate and operate autonomously. The drones in a swarm may be in close or very close proximity to each other or be distant from each other for many kilometers. The key fact is the ability to communicate and share information affecting the execution of a task. The current limitation as to the number of drones in a swarm is the ability to manage information exchange, which will probably be eliminated in the coming years. A drone swarm may consist of many drones of similar or identical size and capabilities, or heterogeneous set of platforms with different weapon and sensor systems. Currently, drone swarms are designed primarily as platforms with sensors, intended mainly for observation and reconnaissance missions (Suzuki, 2018). They are usually composed of small platforms with limited reach. Nevertheless, the dynamic technological progress causes a drone swarm to include much larger platforms with a greater range of use and the possibility of carrying a large amount of weapons. In other words, a drone swarm will become more and more advanced (thanks to improved control algorithms, increased payload, range and flight duration). The differentiation of roles in heterogeneous a drone swarm brings many benefits. Combat drones carry weapon, reconnaissance drones use advanced sensors to track potential targets and detect threats. In turn, communication drones provide stable communication links inside the swarm and in the chain of command. Dummy drones can focus enemy fire on themselves, generating a false radar image. The composition of a drone swarm will depend on the specifics of a given mission and may be modified depending on the nature of the operating environment. The distinction of roles in a drone swarm allows for more complex behavior of the swarm as a whole. As a part of the swarm, multi-task teams can be created cooperating with each other, ensuring the implementation of a wide range of reconnaissance and combat missions (Ekelhof & Paoli, 2020).

The individual drones in a swarm are typically: autonomous, situated in the environment which can act to modify it, capable of sensing their local environment and other nearby drones, able to communicate (locally) with other drones, unaware of the global state of the environment (and other drones), able to cooperate with other robot to perform a given task (s). Based on a study conducted by Arkin (2009), we can distinguish some of the advantages of multi-robotic systems (such as drone swarms) comparing to single robot systems (a single drone) Firstly, improved performance – if tasks are decomposed and execute in parallel, groups will achieve tasks more efficiently. Then, task enablement: just like in nature, a group of drones (swarm) will enable the implementation of tasks that cannot be performed by individual drones. Next, as a part of distributed sensing, a drone swarm will form a "sensor grid" more effectively, which will allow for more information than in the case of a single drone (Kallenborn, 2020). In turn, a distributed action, through parallel, coordinated actions of a large number of drones, will enable conducting of tasks in different places at the same time. What is more, fault tolerance is much greater in a drone swarm than in the case of single unmanned aerial vehicles. The failure of a single drone does not affect the implementation of a task throughout the swarm (Johnson, 2020). On the other hand, Arkin (2009) describes some disadvantages or challenges related to multi-robotic systems as well.

In the case of imperfect technology, the operation of individual drones may disrupt the functioning of the entire swarm (e.g. collisions, loss of communication), which may affect accomplishing a mission. In assumptions, the operation of a drone swarm is autonomous. However, there are concerns about the lack of cooperation and coordination, which may result in competition instead of cooperation in the implementation of specific tasks. These actions may result in uncertainty concerning other robots' intentions.

A large number of unmanned aerial vehicles carrying out a joint mission does not mean that they use swarm tactics. One should distinguish the operation of unmanned aerial platforms used on massive scale (in large numbers), which do not use communication within the group and are not autonomous. Their actions are coordinated by one or more operators (decision makers) in real time or in advance based on programmed behaviors (Ilachinski, 2017). The tactics of using a drone swarm distinguishes it from the massive use of unmanned aerial vehicles as well. John Arquilla and David Ronfeldt (2000, p. 45) define tactical swarming as "seemingly amorphous, but it is a deliberately structured, coordinated, strategic way to strike from all directions at a particular point or points, by means of a sustainable pulsing of force and / or fire, close-in as well as from standoff positions". Drone swarms are highly suited for employing swarming tactics, but do not necessarily need to do so. The members of a drone swarm rapidly share information and coordinate their actions, enabling them to attack from all directions. The ability of drones within a swarm to act either individually or collectively also enables drones to concentrate or disperse as needed.

A drone swarm owns specific attributes distinguishing it from the typical use of unmanned aerial vehicles. To begin with, drone swarms should be self-directed and self-governed. This is achieved through complex behavior, which is the result of combining a few simple behaviors and their interaction with the environment. The natural conclusion is that a drone swarm with planned mission goals must also possess autonomy. Amongst many attributes indicated in literature (See: Sterritt & Hinchey, 2005; Truszkowski et al., 2006), such as self-optimizing, self-healing and self-protecting, development of a future drone swarm capabilities should focus on four issues. First, the size of the swarm. As a rule, the more drones in a swarm, the greater its capabilities. For example, they can search and identify objects over a larger area. Huge number of drones in a swarm increases its survivability in the event of an attack, as losing parts of it will not significantly affect the tasks conduct throughout the whole swarm. On the other hand, building a large drone swarm requires, above all, the ability to handle huge amounts of information. More drones mean more inputs that can influence swarm behavior and decisions. And on a basic level, more drones mean a greater risk of one drone colliding with another. Of course, the size of a drone swarm will depend on the nature of the mission. Stealth missions do not require thousands of drones. In certain cases, a large number of drones can unnecessarily attract the attention of defenders.

Second, diversity. A drone swarm does not have to be of the same type and size of unmanned aerial vehicles, but it can contain both large and small drones equipped with different capabilities. The combination of various sets of drones creates an echelon that is more effective than the individual parts, contributing to synergy effect. Currently, drone swarms mainly consist of small, identical drones, but in the future there will be multi-domain swarms working with other systems in the air, on the water and on the ground. For example, a flying drone will map the area and the ground drone will use this information to plan its operations. A drone swarm can play different roles depending on their various capabilities. Some drones will attack the target, while sensor-based drones will collect battle damage assessment and forward this information to the command post. In turn, communication drones ensure the integrity of communication within a swarm. Small drones with sensors can provide reconnaissance for larger unmanned aerial vehicles by gathering information

about targets and transmitting it to the drone for air strike. A drone swarm can contain unmanned aerial vehicles of various sizes, optimized for different types of targets. A swarm aimed at suppressing enemy air defenses could include drones equipped with anti-missile kits to defeat ground defense, while other drones could be armed with air-to-air missiles to counter enemy aircraft. Cheap dummy drones may turn out to be an extremely valuable complement to a swarm mission, focusing the enemy's defense on themselves and providing freedom of action for more advanced drones. The key, however, is that diversity enables more complex behaviors.

Third, self-configurability. Customizable swarms offer commanders flexibility by allowing them to add or remove drones as needed, and it also allows the swarm to be tailored to the needs of a specific situation or mission. The commander can also change the capabilities of the swarm by adding drones equipped with various sensors, weapon or other capabilities. In extreme cases, a customizable drone swarm could merge into one large unit. This would enable a quick and decisive response to the changing dynamics of combat operations. For example, a small group of drones could draw apart from the larger mass to investigate a possible enemy aircraft. If the new target poses a serious threat, the full swarm may reconfigure itself to attack the identified enemy.

Fourth, self-perfection. A drone swarm is prone to electronic disturbances due to the need for continuous communication between individual units – on which the capabilities of the entire swarm depend. The inability to share information due to disruptions means that a drone swarm cannot function as a coherent whole. The vulnerability to electronic impact depends on the composition of a drone swarm. The swarm may contain drones specifically designed to counteract disruptions. Communication drones can serve as relays to share information, provide alternative communication channels, or simply detect possible jamming and issue withdrawal commands. A drone swarm could also include drones equipped with anti-jamming systems.

3. Key factors influencing a drone swarm employment in military operations

3.1. Operational factor: the scope of drones (swarm) employment in military operations

Basically, drones can be utilized (Figure 1) in an adaptable way in conducting tasks such as intelligence, surveillance, target acquisition, and reconnaissance missions. More specifically, they are used in strikes against surface targets, relaying of information over-the-horizon, Electronic Warfare, Combat Search and Rescue operations, Chemical, Biological, Radiological and Nuclear Warfare threats motoring, payloads and logistics transportation. Drones are presumed to provide their services at any time, be reliable, automated and autonomous. They may store a wide range of information from troop movements to environmental data and strategic operations.

From doctrinal point of view, based on NATO solutions, unmanned aircraft may be categorized into three classes, and the division criterion is the maximum take-off weight of the unmanned aircraft (NATO Standardization Office, 2020). The first class includes unmanned aerial vehicles up to 150 kg, class II 150–600 kg, class III over 600 kg. The adopted classification adjusts individual classes to command levels and assigns them specific tasks. Drones can be also divided as strategic, operational, and tactical. Strategic drones are used for long-range reconnaissance over hostile territory. They include systems like the Global Hawk, which can cruise at 20,000 meters above sea level for 40 hours and travel 3,000 nautical miles. Operational drones include the Predator and Reaper systems, which can fly at 7,500

and 15,000 meters respectively. They are deployed at the theatre level of combat and can be used for both reconnaissance and attack purposes. Lastly, tactical drones are low altitude, short range aircraft (20 miles or less). An example is the Dragon Eye system. Unlike strategic and operational drones, which can be either remotely piloted or preprogrammed to fly autonomously, tactical drones are fully operator-controlled (Willis et al., 2021).

Cass I of unmanned aircraft (micro, mini, small) are primarily used by land forces and special forces. Land forces use them to conduct reconnaissance in the close tactical area, in order to improve situational awareness of a given subunit. Additional tasks from this class may be mark a target and support artillery operations by airborne adjustment of fire. Class I mainly supports operations conducted by ground forces from the platoon level to the battalion. Similar tasks will be carried out by special forces subunits. However, most unmanned aircraft are micro and mini class – highly mobile and simple to use, suitable for use in combat environment.

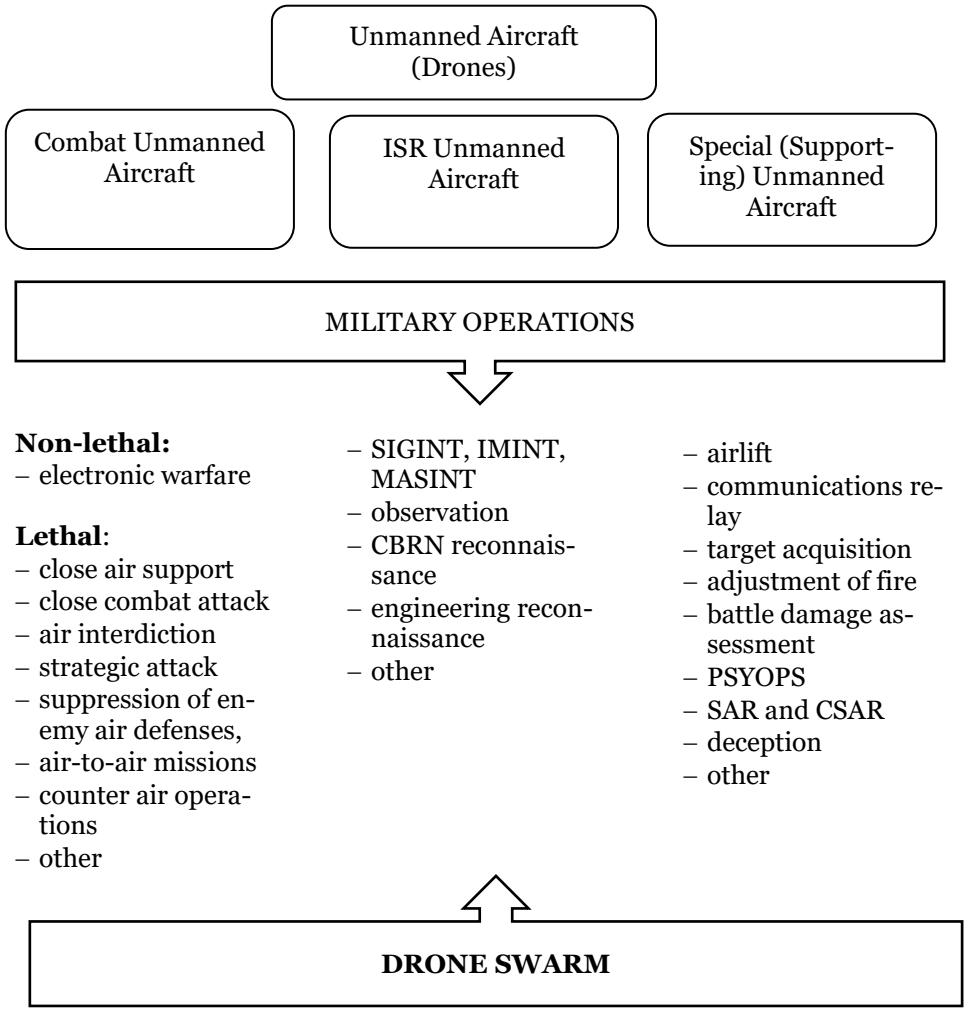

Figure 1. Unmanned Aircraft Systems employment in military operations. Own work.

Naval forces use mini and small unmanned aircraft of Class I, mainly VTOL (Vertical Take Off and Landing). They are capable of operating from the decks of ships. Their main task is to supervise and control sea areas as well as participate in searching and identifying of enemy submarines and surface ships. The naval force may also be equipped with land-based Class I (small) of unmanned aircraft that are part of the maritime reconnaissance

squadron. Their tasks is similar to those presented above, including the protection of sea bases (ports).

Class II of unmanned aircraft are mainly short- and medium-range tactical aircraft conducting tasks at the brigade and division level. They carry out reconnaissance and observation missions at distances ensuring a given level of command in decision-making of. The prospective development of dedicated devices (sensors) does not exclude their use for other tasks, e.g. close combat attack. Tactical unmanned aircraft can also be used by naval forces from land based airfields to conduct reconnaissance of sea basins.

Class III of unmanned aircraft is used mainly by the Air Force. Their size and maximum take-off weight force them to operate from air bases (airports) with prepared infrastructure. These are MALE (Medium Altitude Long Endurance) and HALE (High Altitude Long Endurance) systems, which may be armed. These platforms carry out tasks over theater of operations supporting land, sea, special and air forces. The main task conducted by class III of unmanned aircraft is airspace surveillance and early warning. The information (data) obtained has an impact on decision making at the Joint Forces Command level. Like manned aviation, they can also conduct air strikes against targets selected in targeting process or close air support and air interdiction.

One can assume that in the next decade, leading military powers as well as non-state actors will be equipped with a drone swarm. A drone swarm will be a cheaper equivalent of advanced and much more expensive weapon systems including typical unmanned aircraft. They will be used to destroy ground targets, but their effectiveness will probably also be proven in air-to-air operations – against enemy aircraft or its drone swarms. New means of transporting and launching them will be implemented, based on both ground vehicles, aircraft (manned and unmanned), as well as individual soldiers' equipment.

From a doctrinal point of view, a drone swarm can be used for several types of military operations. First, it will ensure a dispersed distribution of sensors responsible for reconnaissance, observation, tracking, precise location and tracing. This can be done both actively and passively. For instance, multiple widely distributed sensors can locate emitters by comparing the differences in time of arrival and frequency due to the Doppler shift from relative movement. For active detection, distributed sensors can operate like a multi-static radar, with one sensor emitting a radar pulse and multiple sensors detecting the reflection, allowing stealthier and higher-quality radar detection (Martinic, 2020).

Second, a drone swarm will provide offensive actions in the form of kinetic attack or an attack using electronic warfare kits. It will be able to affect many enemy targets, attacking them with their weakest defense. Acting in a distracted manner it will hinder the defender's reaction. If ten drones attack a target simultaneously and seven are shot down, three will still be able to accomplish their mission. Presumably, in the future even a large drone swarm will be more effective and less costly to use compared to single manned or unmanned aerial vehicles.

Third, a drone swarm will be used for defensive operations, misleading (deception) the opponent as to the size and number of the combat group in the air and counteracting his attack. Scharre (2014) describes how miniature air-launched decoys can be used to fool enemy radars. He also notes that large numbers of drones could swarm over an enemy's airfield to prevent aircraft from taking off. A similar tactic could be used to protect a piece of territory from overflights by enemy helicopters or airplanes, though the difficulty of such a mission would increase with the size of the area that needed protecting.

Drone swarms in combat operations can be directed against targets that require a small amount of explosives: helicopters at landing areas, planes at airports, fuel tanks or elements of transmission and communication systems. Hundreds or even thousands of drones in the area of operations may engage enemy combat systems, blocking the ability to conduct their

tasks (Rossiter, 2018). Moreover, electronic interference by the enemy with a large number of drones in the swarm will not bring the desired effects.

3.2. Technical factor: Command and Control models of a drone swarm

As Scharre (2014) notes, in recent years the concept of coordination of activities between multiple vehicles (objects) has been tested in simulations and experiments all over the world. Hence, it can be concluded by analogy that the use of a drone swarm to a certain extent is technically possible today.

Referring to command and control (C2) models, Scharre (2014) believes that the implementation of effective command and control over a swarm is a relatively new research area in which the concept of decentralized swarm management is considered to be the essence of its functioning.

Scharre's (2014) model includes four distinctly different C2 swarm architectures (Figure 2):

- Centralized control model: the swarm elements feed information back to a central planner which then tasks each element individually.
- Hierarchical control model: the individual swarm elements are controlled by "squad" level agents, which are in turn controlled by higher level controllers, and so on.
- Coordination by consensus model: the swarm elements communicate to one another and converge on a solution through voting or auction-based methods.
- Emergent coordination model: the coordination arises naturally by individual swarm elements reacting to others, like in animal swarms.

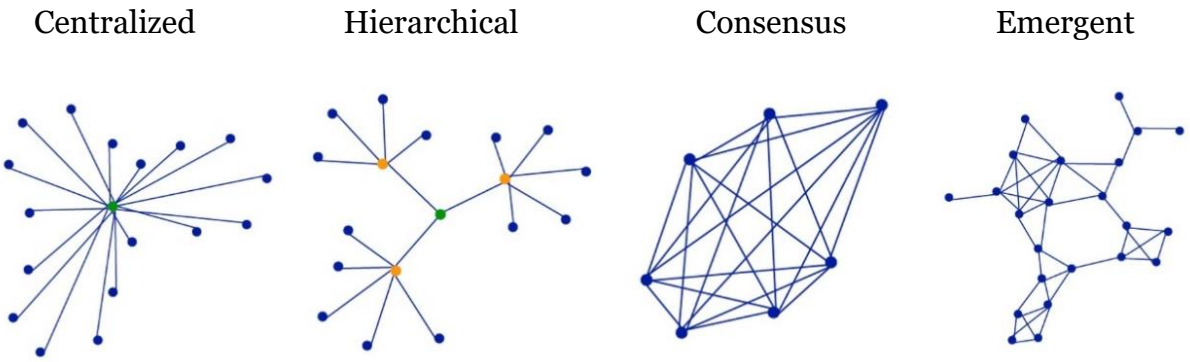

Figure 2. C2 swarm architectures. Adopted from: "Robotics on the Battlefield, Part II: The Coming Swarm" by P. Scharre. Copyright 2014 by Center for a New American Security.

As far as practice is concerned, the presented models can be applied to command a squadron of combat aircraft. The centralized control model imitates a fighter squadron. Pilots can communicate with each other, but their mission is coordinated centrally by a command post on the ground. Therefore, the degree of autonomy of individual pilots is limited. In line with the hierarchical control model, the squadron commander's superiors set the overall directions for the mission, but the squadron commander retains a certain degree of autonomy to actually carry it out (Grimal & Sundaram, 2018). There is a noticeable difference related to coordination by consensus model. The drones would have autonomy in making decisions among themselves within the swarm, while the squadron of manned aviation would be dependent on the final decisions of the ground control, even though pilots may of course communicate with each other during the mission. Finally, the emergent coordination model which is unique in terms of intuitiveness because there is no need to communicate

with ground control. This model indicates that the drone swarm is much more complex than the fighter squadron. It is likely that highly trained manned air squadron pilots may act in a similar way, but the level of intuition about how a squadron works as a group during a mission is definitely lower than in a drone swarm.

Specifying the presented C2 models of a drone swarm, in a centralized control model the chain of command is relatively simple, comparable to a uncomplicated command system. According to Burdick (2015), the lead drone assigns tasks to the drones in the swarm, and all nodes are identical. The choices of the leading drone, treated as a commander, depend on its current position, combat situation and other current factors affecting the execution of the task. If the lead drone cannot assign the accomplishment of tasks, it may be replaced by another node so that the mission can continue.

The hierarchical control model is based on a system of nodal points. Each node in turn controls multiple subsets in the swarm, which in turn can also be nodes. This model replicates the traditional C2 military structure. If any node is eliminated, the next one takes over, maintaining continuity of command and situational awareness. The commanding node is responsible for creating a big picture plan which is transmitted hierarchically and tactical details are added by subordinate nodes. This means that at the beginning of each operation, the main (lead) drone determines the battle plan and search pattern, including the number of drones necessary to accomplish the mission. Moreover, it entrusts each drone with a specific task to conduct (Grimal & Sundaram, 2018).

The coordination by consensus model, referred to as a distributed drone swarm, allows the swarm to operate without a perceptible constant linkage command-individual drones in the swarm. In certain situations, the drones in the swarm can independently decide on the way of conducting the mission. They can stick to the original plan or change it to successfully complete their mission. In other words, all decisions are made by consensus (Chen, Tang & Lao, 2020).

The fourth, emergent coordination model is a conceptual challenge. As with coordination by consensus model, there is no apparent chain of command. The swarm operates “organically” adjusting to the current situation shaped by external elements, not a predetermined course of action. The operation of a drone swarm is intuitive, focused on independent decision making, reliant on changes in the environment in which they operate (Grimal & Sundaram, 2018). The value of the emergent C2 model is that it extends range, decreases bandwidth, and allows the swarm to dynamically scale in size. This means that the geographic coverage area of a swarm weapon using an emergent C2 model is significantly larger than either a consensus or a centralized model (McLaughlan & Hexmoor, 2011).

3.3. Human factor: dilemmas of a drone swarm autonomy

The use of an appropriate C2 model in drone swarm operations is directly related to the level of autonomy of the entire system. In the case of defining autonomous systems, the most common approach includes the criterion of the degree of human control over a machine (human-machine relation). This categorization distinguishes semiautomatic systems ("human in the loop"), in which the automatic operation is possible until a certain moment and then human intervention is necessary. The second group covers supervised systems ("human on the loop"), in which there is a possibility of uninterrupted autonomous operation, but with the possibility of human intervention at any given moment. Weapon systems from this group are able to select and combat targets on their own, from the moment they were activated. However, the operator of such weapon system has the knowledge about what kind of objects can be targeted and the operator may intervene at any time by interrupting the process. In practice, these types of weapon systems (supervised) are used in defensive operations and in undemanding operational environment. They react directly to the defined

threats, where the reaction of a human (operator) could be too slow, and in the case of doubtful situations the operator may react at any time. The third group consists of fully autonomous systems ("human out of the loop"), without the possibility of human intervention. They refer to weapon systems that independently, without human participation, are able to select and combat targets in a previously defined geographical region, time interval and according to the adopted rules. The operator does not know what targets will be selected for combating, but it should be remembered that the types of combated objects have been previously defined by a human according to the specific criteria. In other words, a man decides earlier in what manner the autonomous combat system will carry out its tasks (OUSD(A&S), 2018).

In the case of using a drone swarm in military operations, it is desirable to employ the emergent coordination model based on full autonomy. However, while full autonomy offers clear benefits for drone swarms, clear risks exist too.

More autonomous drone swarms are easier to control. Autonomy can allow multiple drones in a swarm to follow a single leader, maintain constant distances from each other, avoid obstacles, and launch attacks against targets. Each function automized is one less function requiring operator attention. Larger, more complex swarms of drones place greater cognitive demands on human operators. Large swarms have greater operational requirements and more sensors to send information to operators. Overworked operators may react slower. Heterogeneous swarms of drones of various sizes and payloads require even more attention. Operators must coordinate complex activities, such as deploying one drone to search for targets and the other to conduct attacks (U.S. Department of Defense, 2017).

Even assigning humans alone to make decisions about the use of force would be a challenge as the size of the swarm grows due to the large amount of inputs. An operator must be aware of input signals from multiple sensors in the remote area. While many operators could be used to control a swarm of drones, this would offset any cost benefits. In a military context, an operator must also detect, avoid and counter potential enemies. Any delays in communication between drones and an operator increase the risk of enemies overcoming the swarm. Since drone swarms are essentially information-dependent weapons, enemies can attack the communication systems between drones, and between drones and the operator (Scharre, 2016).

Greater autonomy can ensure greater survivability. A swarm of human-controlled drones would be at risk of losing the operator. In the case of a swarm of human-controlled drones, the human is the weakest point as killing or incapacitating the operator would deactivate the swarm. A human operator may also become sick or injured unrelated to an enemy attack. A fully autonomous drone swarm does not face such threats. Greater autonomy also allows a drone swarm to make decisions faster. In the case of a remotely controlled drone swarm, an operator must receive information from drones in the field, interpret this information, decide to use sensors or weapons, and issue the command to fire against targets. Delay can cause the enemy to open fire first, change position, or take any other defensive action. Delay will be even greater when there are more drones in the swarm as the operator can focus on a different location. Delegating decision making to artificial intelligence in the field can shorten the decision-making loop and thus increase the swarm's survivability and ability to cause harm. Greater autonomy also enables innovative use of a drone swarm. It can be programmed to carry out multiple attacks over a longer period, dispersed between attacks (Defense Science Board, 2016).

On the other hand, concerns about losing control of a drone swarm must be taken into account. An uncontrolled a drone swarm has the potential to kill friendly civilians or military personnel simply because of an algorithm error. There are concerns about possible violations of international law of armed conflict in places where it is planned to use of autonomous systems, including a drone swarm. Giving full control to artificial intelligence could

create new security gaps that undermine the reliability of a drone swarm. By its nature, full autonomy requires software and / or hardware to assist in making more sophisticated decision making. It is software and / or hardware that can make mistakes or adversaries can introduce errors through a cyber-attack. The complexity of the system can make it difficult to identify intentional or random errors. Lack of human control can exacerbate these fears into the belief that they are unexpected or uncontrollable (Wallach, 2017). There are also more mundane concerns. Military services may have cultural inhibitions before granting full autonomy to drone swarms. Long-term bans are especially likely if systems are unreliable. Full autonomy may just not be worth it. Nevertheless, due to the potential benefits, it is certainly possible for the state or the military to recognize that the benefits of using autonomous drone swarms outweigh the costs.

4. Conclusions

The architecture of a drone swarm should be based on artificial intelligence and machine learning algorithms. Drone's ability to communicate with each other within a swarm is a feature that distinguishes them from typical use of unmanned aerial vehicles. A drone swarm should be built from as many unmanned aerial vehicles as possible with comparable qualities. The utilization of artificial intelligence will allow to assign tasks inside the swarm to individual drones, which will increase the probability of conducting missions. In the future, an emergent coordination model will be optimal for a drone swarm command and control. It will be based on natural behaviors of swarms occurring in nature, such as a swarm of bees, birds or a school of fish. In this model, there will be no classic chain of command, and a drone swarm will be adaptive and intuitive, making decisions depending on a given tactical situation. The specific attributes of a drone swarm that distinguish it from typical use of unmanned aerial vehicles include size, diversity, self-configurability and self-perfection.

Currently, it is difficult to predict new types of military operations unique to a drone swarm. It should be assumed that these will be typical operations conducted today by unmanned aerial vehicles. These contain: intelligence, surveillance and reconnaissance operations, distributed offensive operations and defensive operations. However, attributes of a drone swarm suggest that these operations will be carried out more safely and faster with minimal (human on the loop) or without human intervention (human out of the loop).

There is a need for further research on the autonomy of a drone swarm. Despite the undoubted advantages associated with the use of full autonomy in conducting tasks by a drone swarm, there are also concerns about some uncontrolled, independent carry out of tasks by them without human intervention in a manner that is illegal. Research into artificial intelligence and machine learning may partially solve these issues. However, the decision to employ a drone swarm for a specific task should be left to humans, and should also be exercised constantly during the mission.

All in all, despite the dynamic development of drone technologies, an expectancy of application a drone swarm in combat operations seems to be distant so far. Public shows are not swarms, as they perform a programmed procedure based on a defined algorithm. Likewise, the aforementioned attacks on the Russian airbases, the Syrian military convoy and the Saudi oil fields were not drone swarms. These were coordinated strikes involving a large number of drones which did not communicate or cooperate in carrying out the mission. They can currently be defined as a drone proto-swarm. However, technology is constantly evolving and software is available on the market. At this stage, no state or non-state entity is able to operate a drone swarm in combat operations. In turn, military experiments in this field

are carried out in simplified environments, with the use of relatively small swarms and limited communication equipment (sensors) on board. The main limitation is the equipment that determines the size, weight, battery power and on-board computers, which in turn translates into the communication capacity between the swarm and its operator.

Declaration of interest – The author declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this article

References

1. Arkin, R. (2009). *Governing Lethal Behavior in Autonomous Robots*. Taylor and Francis Group Publishing.
2. Arquilla, J., & Ronfeldt, D. (2000). *Swarming and the Future of Conflict*. RAND Corporation. https://www.rand.org/content/dam/rand/pubs/documented_briefings/2005/RAND_DB311.pdf
3. Burdick, J.E. (2015). *Instantly Basing Locust Swarms. New Options for Future Air Operations (Drew Paper No. 20)*. AU Press. https://media.defense.gov/2017/Nov/21/2001847261/-1/-1/0/DP_0020_BURDICK_INSTANT_BASING_LOCUST_SWARMS.PDF
4. Chen, X., Tang, J., & Lao, S. (2020). Review of Unmanned Aerial Vehicle Swarm Communication Architectures and Routing Protocols. *Applied Sciences, 10*(10:3661). https://doi.org/10.3390/app10103661
5. Defense Science Board (2016). *Report of the Defense Science Board Summer Study on Autonomy*. Department of Defense, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. https://www.hsdl.org/?view&did=794641
6. Ekelhof, M., & Paoli, G.P. (2020). *Swarm Robotics. Technical and Operational Overview of The Next Generation of Autonomous Systems*. United Nations Institute for Disarmament Research. https://unidir.org/sites/default/files/2020-04/UNIDIR%20Swarm%20Robotics%20-%202020.pdf
7. Grimal, F., & Sundaram, J. (2018). Combat Drones: Hives, Swarms, and Autonomous Action? *Journal of Conflict & Security Law*, *23*(1), 105–135. https://doi.org/10.1093/jcsl/kry008
8. Ilachinski, A. (2017). *AI, Robots, and Swarms. Issues, Questions, and Recommended Studies*. CAN Corporation. https://www.cna.org/cna_files/pdf/DRM-2017-U-014796-Final.pdf
9. Johnson, J. (2020). Artificial Intelligence, Drone Swarming and Escalation Risks in Future Warfare. *The RUSI Journal, 165*(2), 1–11. https://doi.org/10.1080/03071847.2020.1752026
10. Kallenborn, Z. (2020). *Are Drone Swarms Weapons of Mass Destruction? (Future Warfare Series No. 60)*. AU Press. https://media.defense.gov/2020/Jun/29/2002331131/-1/-1/0/60DRONESWARMS-MONOGRAPH.PDF

11. Martinic, G. (2020). Swarming, Expendable, Unmanned Aerial Vehicles as a Warfighting Capability. *Canadian Military Journal*, *20*(4), 43–49. http://www.journal.forces.gc.ca/vol20/no4/PDF/CMJ204Ep43.pdf
12. McLaughlan, B. & Hexmoor, H. (2011). Emergent command and control architecture for dynamic agent communities. *Journal of Experimental & Theoretical Artificial Intelligence*, 23(4), 363–387. https://doi.org/10.1080/09528130701664608
13. NATO Standardization Office (2020). *ATP-3.3.8.2 Unmanned Aircraft System Tactics, Techniques And Procedures*. NATO Standardization Office. https://nso.nato.int/nso/
14. OUSD(A&S) (2018). *Unmanned Systems Integrated Roadmap 2017–2042*. United States. Office of the Under Secretary of Defense for Acquisition and Sustainment. https://www.defensedaily.com/wp-content/uploads/post_attachment/206477.pdf
15. Rossiter, R. (2018). Drone usage by militant groups: exploring variation in adoption. *Defense & Security Analysis,* 34(2), 113–126. https://doi.org/10.1080/14751798.2018.1478183
16. Scharre, P. (2014). *Robotics on the Battlefield, Part II: The Coming Swarm*. Center for a New American Security. https://www.files.ethz.ch/isn/184587/CNAS_TheComingSwarm_Scharre.pdf
17. Scharre, P. (2016). *Autonomous Weapon and Operational Risk*. Center for a New American Security. https://s3.amazonaws.com/files.cnas.org/documents/CNAS_Autonomous-weapons-operational-risk.pdf
18. Sterritt R., & Hinchey, M. G.(2005). Apoptosis and self-destruct: A contribution to autonomic agents? In Hinchey, M.G., Rash, J.L., Truszkowski, W.F. & Rouff, C.A. (Eds.), Formal Approaches to Agent-Based Systems (pp. 269–278). Springer. https://www.springer.com/gp/book/9783540244226
19. Suzuki, S. (2018). Recent researches on innovative drone technologies in robotics field. *Advanced Robotics, 32*(19), 1008–1022. https://doi.org/10.1080/01691864.2018.1515660
20. Tan Y., & Zheng, Z. (2013). Research Advance in Swarm Robotics. *Defence Technology*, *9*(1), 18–39. https://doi.org/10.1016/j.dt.2013.03.001
21. Truszkowski, W. F., Hinchey, M. G., Rash, J.L. & Rouff, C. A. (2006). Autonomous and autonomic systems: a paradigm for future space exploration missions. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews),* 36(3),279–291.https://doi.org/10.1109/TSMCC.2006.871600
22. U.S. Department of Defense (2017). *Directive 3000.09: Autonomy in Weapon Systems*. U.S. Department of Defense. www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300009p.pdf.
23. Wallach, W. (2017). Toward a Ban on Lethal Autonomous Weapons: Surmounting the Obstacles. *Communications of the ACM*, *60*(5), 28–34. https://doi.org/10.1145/2998579
24. Willis, M., Haider, A., Teletin, D.C., Wagner, D. (2021). *A Comprehensive Approach to Countering Unmanned Aircraft Systems*. Joint Air Power Competence Centre. https://www.japcc.org/wp-content/uploads/A-Comprehensive-Approach-to-Countering-Unmanned-Aircraft-Systems.pdf