Mini-Drone Swarms: Their Issues and Potential in Conflict Situations

M Lehto[1], W Hutchinson[2]

[1] *University of Jyväskylä*
Finland

Email: martti.j.lehto@jyu.fi

[2]*Security Research Institute*
Edith Cowan University
Perth, Australia

Email: w.hutchinson@ecu.edu.au

Abstract: *Drones are currently used for a wide range of operations, such as border surveillance, general surveillance, reconnaissance, transport, aerial photography, traffic control, earth observation, communications, broadcasting, and armed attacks.*

This paper examines the swarming and associated abilities to overwhelm a combatant as well as bring extra functionality by means of extra sensors spread throughout the swarm. The strategy of stealth is becoming increasingly less effective. Combatants can not only sense them, but can also successfully destroy them (although this cannot be said for nano-drones). For mini-drones, objectives can be enhanced by the strategy of overwhelming.

Keywords: *Drone, Security, Artificial Intelligence, Swarming, Surveillance, Suicide Drones, Networks, Autonomous Drones, Lethal Autonomous Weapons (LAWs)*

Introduction

There is no one standard when it comes to the classification of Unmanned Aircraft Systems (UASs), sometimes called Unmanned Aerial Vehicles (UAVs). Defence agencies have their own standard, and civilians have their ever-evolving loose categories for UASs. People classify them by size, range, and endurance and use a tier system that is employed by the military. A UAS is a "system whose components include the necessary equipment, network, and personnel to control an unmanned aircraft" (Department of Defense [DoD] 2014). In some cases, the UAS includes a launching element (DoD 2014).

Papireddy defines Unmanned Aircraft as a powerful system, that does not carry a human operator, that uses aerodynamic forces to provide vehicle lift, that can fly autonomously or be piloted remotely, that can be expendable or recoverable, and that can carry a payload (2015). The International Civil Aviation Organization (ICAO) employs the acronym RPAS (Remotely Piloted Aircraft System) for "A remotely piloted aircraft, its associated remote pilot station(s), the required command and

control links and any other components as specified in the type design" (ICAO 2019). As the world pioneer in the creation and implementation of regulations for the use of commercial Unmanned Aerial Vehicles, the French Directorate for Civil Aviation (DGAC) sees commercial UAVs as drones. In a general way, many countries use the term 'drone'. For many, UAV is used mostly in a military context, so 'drone' covers both civil and military (Altigator Unmanned Systems 2019).

This article uses the term 'drone' to cover the whole spectrum of aerial unmanned vehicles. It should be noted that this paper, concentrates on the aerial environment. However, drones have been produced for other environments, such as underwater, terrestrial, maritime, and space, as well as various environments hostile to humans (for instance, radioactive, chemically affected, and highly infectious areas). These environments will be brought up in the latter part of the paper where general issues surrounding drones will be discussed. The concept of swarming, which has changed the nature of drone use and effectiveness, is also highlighted.

Categories

Unmanned Aircraft Systems (UASs) can be roughly divided into fixed and rotary wings. Multi-rotor helicopters are referred to as multi-copters. Other classification elements include size, Maximum Gross Takeoff Weight (MGTW), range, and endurance. For combat, there are two main groups: Unmanned Combat Aerial Vehicles (UCAVs) and Unmanned Combat Aerial Rotorcrafts (UCARs). These can be categorized by performance and combat mission.

Multi-rotor multi-copters powered by an electric power source are manufactured with various numbers of engines. Most used are

- Quadrocopter (4 propellers, vertically oriented),
- Hexacopter (6 propellers, 6-angle, symmetrically mounted),
- Oktocopter (8 propellers, either 4 or 8 angles symmetrically mounted, in 4-angle installation, with the motors arranged in pairs on top of each other).

Table 1, below, illustrates classifications according to the U.S. Department of Defense (DoD) (Pennsylvania State University 2019).

Category	Size	Maximum Gross Takeoff Weight (MGTW) (kg)	Normal Operating Altitude (ft)	Airspeed (knots)
Small UAV Mini, Micro, Nano UAV	Length 15 cm - 2 m Nano UAVs can also be smaller	0-9	<1,200 ft Above Ground Level, AGL	<100
Medium UAV	5-10 m	9-25	<3,500 AGL	<250

Large UAV	> 10 m	<600	<18,000 Mean Sea Level	<250
Larger UAV	> 10 m	>600	<18,000 MSL	Any airspeed
Largest UAV	> 10 m	>600	>18,000 MSL	Any airspeed

Table 1: UAV classification according to the U.S. Department of Defense

Table 2, below, illustrates classification according to range and operating time (Pennsylvania State University 2019).

Category	Range (km)	Operating time
Very low close-range UAV	5	20-45 min
Close range UAV	50	1-6 hours
Short range UAV	> 150	8-12 hours
Mid-range UAV	< 1000	12-24 hours
Endurance UAV	> 10 000	24-36 hours

Table 2: UAVs classification according to range and operating time

In the late 1990s, the U.S. Armed Forces produced a classification according to the information of the UAV system provided to different user levels. This classification is shown in **Table 3**.

UAV	Capability
Micro Unmanned Aerial Vehicle (MUAV)	Producing information within a radius of less than 100 kilometres from its land station.
Tactical Unmanned Aerial Vehicle (TUAV)	Producing information within a radius of about 200 kilometres of its land station.
Medium Altitude Endurance Unmanned Aerial Vehicle (MAE)	Producing information within a radius of about 750 kilometres of its land station.
High Altitude Endurance Unmanned Aerial Vehicle (HAE)	Producing information for long-term and near-real-time information for the control of large areas.

Table 3: UAV clasification based capability

One group consists of UAVs which are focused on combat:

- UCAV, Unmanned Combat Aerial Vehicle;
- UCAR, Unmanned Combat Aerial Rotorcraft

UACV	Performance	Combat mission
Deep Penetration RPAS	Designed for full electromagnetic stealth	Designated to conduct reconnaissance and air strikes deep inside enemy territory
Combat RPAS	Designed for high G-forces and manoeuvrability	Designated to conduct air-to-air and air-to-ground combat in non-permissive and hostile air environments
Swarm RPAS	Forming a swarm	Designed for expendability and operating in large numbers
Carrier RPAS	Designed to carry an immense stock of long-range	Precision-guided air-to-air and air-to ground munitions, designed to project military power like naval aircraft carriers

Table 4: UCAV classification based on combat missions

Over the past two decades, Remotely Piloted Aircraft Systems (RPASs) have been fielded in increasing numbers across many nations and military services. It is very unlikely there will be a 'one-size-fits-all' solution for RPAS operations in a contested environment. In addition, Reconnaissance RPAS are expected to be upgraded and to continue the role of current Medium-Altitude Long-Endurance (MALE)/ High-Altitude Long Endurance (HALE) systems (JAPCC 2014).

Table 4, above, illustrates UCAV classification based on combat missions (Joint Air Power Competence Centre [JAPCC] 2014).

Drone Autonomy

Autonomy allows the reduction of the frequency at which the operators must interact with the drone supporting the implementation of more robust system solutions, where the role of the operators is to manage and to supervise, through appropriate human machine interface, the command and control functions without direct interaction.

There are various ways to discuss autonomy in weapon systems. Although precise definitions are critical for design and engineering purposes, understanding the debate about autonomy requires an acknowledgement of these differing uses of the term, typically centred on ethically relevant subprocesses of the system as a whole: targeting, goal-seeking, and the initiation of lethality (Payne 2017).

According to the U.S. DoD (2018), 'autonomy' is defined as the ability of an entity to independently develop and select among different courses of action to achieve goals based on the entity's knowledge and understanding of the world, itself, and the situation. Autonomous systems are governed by broad rules that allow the system to deviate from the baseline. This contrasts with automatic systems, which are governed by prescriptive rules that allow for no deviations. While early robots generally only exhibited automatic capabilities, advances in Artificial-Intelligence (AI) and Machine-Learning (ML) technology have allowed systems with greater levels of autonomous capabilities to be developed. The future of unmanned systems will stretch across the broad spectrum of autonomy, from remote-controlled and automated systems to fully autonomous ones.

Autonomous categories are

> **Human-in-the-loop:** In this mode, humans retain control of selected functions preventing actions by the AI without authorization; humans are integral to the system's control loop.
> **Human-on-the-loop:** The AI controls all aspects of its operations, but humans monitor the operations and can intervene when, and if, necessary.
> **Human-out-of-the-loop:** The AI-algorithms control all aspects of system operation without human guidance or intervention. The autonomous drone engages without direct human authorization or notification.

Autonomy results from delegation of a decision to an authorized entity to act within specific boundaries. An important distinction is that systems governed by prescriptive rules that permit no deviations are automatic, but they are not autonomous. The Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (2014) states that to be autonomous, a system must have the capability to independently compose and select among different courses of action to accomplish goals based on its knowledge and understanding of the world, itself, and the situation. 'Automatic' really means the drone can function alone but only by obeying a set of pre-set rules in response to sensors' inputs.

Drone Military Operations

The development of Unmanned Aerial Vehicles is intensifying as technology becomes cheaper. Drones can be used in a flexible manner in different tasks, such as intelligence, surveillance, target acquisition, and recognition missions, in strikes against surface targets, over-the-horizon relaying of information, Electronic Warfare (EW), Combat Search and Rescue (CSAR), Chemical, Biological, Radiological, and Nuclear Warfare (CBRN), logistic replenishments, and Counter Improvised Explosive Devices (C-IED) in a favourable environment or in areas where the risk level is elevated. In conflict situations, their functions can be changed to a multitude of purposes.

Drones are presumed to provide their services at any time, to be reliable, automatic, and often autonomous. Based on these assumptions, governmental and military leaders expect drones to improve national security through surveillance and/or combat missions. To fulfill their missions, drones need to collect and process data. Therefore, drones may store a wide range of information from troop movements to environmental data and strategic operations. The amount and kind of information needed make drones an extremely interesting target for espionage and, hence, endanger drones through theft, manipulation, and attacks.

Various types of air domination systems are being considered to enable a military force to dominate an area from the air for extended periods and to deny enemy movements and manoeuvring. Unmanned combat aircraft, these purposes can be divided into two categories according to their operating model: loitering or swarming.

In the U.S., current systems under consideration are standard weaponized drones or small expendable loitering weapons fitted with imaging sensors, such as the Low-Cost Autonomous Attack System (LOCAAS). Operating in swarms of 'intelligent munitions' weapons, the LOCAAS can autonomously search for and destroy critical targets, while aiming over a wide combat area.
A loitering weaponized drone (also known as a suicide drone or kamikaze drone) is a weapon

system category in which the weaponized drone or munitions loiters around the target area for some time, searches for targets, and attacks once a target is located. Loitering systems enable faster reaction times against concealed or hidden targets that emerge for short periods without placing high-value platforms close to the target area and allow more selective targeting as the actual attack mission can be aborted.

Drone Civilian Operations

Various UAVs are increasingly being used for various civilian purposes, such as government missions (law enforcement, border security, coastguard), firefighting, surveillance of oil and gas industry infrastructure, and electricity grids/distribution networks, traffic control, disaster management, agriculture, forestry and fisheries, civil engineering, earth observation and remote sensing, and communications and broadcasting. PricewaterhouseCoopers (PwC 2016) estimated the value added to the economy by drones at $127 billion. According to Single European Sky ATM Research (SESAR 2016), the growing drone marketplace shows significant potential, with European demand suggestive of a valuation in excess of EUR 10 billion annually, in nominal terms, by 2035 and over EUR 15 billion annually by 2050.

The development of the civil drone industry is dependent on the ability of drones to operate in various areas of the airspace, especially at very low levels. According to SESAR (2016), "In aggregate, some 7 million consumer leisure drones are expected to be operating across Europe and a fleet of 400,000 is expected to be used for commercial and government missions by 2050".

Critical infrastructure (CI) includes a large variety of elements from nuclear reactors, chemical facilities, water systems, logistics, and airports to healthcare and communications, and now drones are growing a very important part in this critical infrastructure environment. They have numerous tasks in critical infrastructure maintenance and protection. Human work is reduced, and tasks can be performed cost-effectively.

At the same time, CI must deal with the new and emerging threat of drones. The most headline-grabbing risks tend to be those of physical and electronic attacks. For example, drones could carry explosives into a nuclear power plant or get close enough to execute cyberattacks, causing disruptions or mechanical failures or even stealing sensitive data. The low-cost, global proliferation and capabilities of drones weighing less than 20 pounds make them worthy of specific focus. Future adversaries could use these small systems to play havoc with critical infrastructure both in the air and on the ground—thus, necessitating new actions to defend CI assets.

In organized civil disturbances, the availability of mini-drones can be used for surveillance by both law enforcement and those causing the disturbance. Swarming these drones (discussed in the next section) can give a lot of coverage for either side, and a myriad of sensors can provide various data. Also, in disaster events (such as fires, large crashes of many types, or epidemics) they can be used for intelligence and for delivery of such things as drugs; in fact, the variety of functions can be left to the imagination.

Drone Swarming

Various types of air domination systems are being considered to enable a military force to dominate an area from the air (and in the sea, on ground, and in space for that matter) for extended periods and to deny enemy movements and manoeuvring.
'Swarming' is the coordinated use of various drones which might be of different types, 'intelligence',

size, and capabilities so they can act in unison. This use of swarming techniques (where numerous drones are used for one purpose) is of increasing interest. The decreasing cost of smaller drones (Hambling 2015) plus the built-in redundancy of swarms make the use of many drones for an attack much more appealing.

Current systems under consideration are standard weaponized UASs or small expendable loitering weapons, fitted with imaging sensors, such as the Low-Cost Autonomous Attack System (LOCAAS). Operating in swarms of 'intelligent munitions' weapons, the LOCAAS can autonomously search for and destroy critical mobile targets while aiming over a wide combat area (DoD 2014). Along with sensor autonomy, swarming drones will require the ability to self-navigate and self-position to collect imagery and signals efficiently (DoD 2005).

A loitering munition (also known as a suicide drone or kamikaze drone) is a weapon system category in which the munition loiters around the target area for some time, searches for targets, and attacks once a target is located. Loitering munitions enable faster reaction times against concealed or hidden targets that emerge for short periods without placing high-value platforms close to the target area, and allow more selective targeting as the actual attack mission can be aborted. Loitering munitions fit in the niche between cruise missiles and Unmanned Combat Aerial Vehicles, sharing characteristics with both. They differ from cruise missiles in that they are designed to loiter for a relatively long time around the target area, and from UCAVs in that a loitering munition is intended to be expended in an attack and has a built-in warhead.

Drones are currently in widespread use around the world, but the ability to employ a swarm of these systems to operate collaboratively to achieve a common goal will be of great benefit to national defence. A swarm could support lower operating costs, greater system efficiency, as well as increased resilience in many areas.

Drone swarms carry additional communications needs. Effective distributed operations require a battlefield network for drone-to-drone communications to allocate sensor targets and priorities and to position aircraft where needed. While the constellation of sensors and aircraft needs to be visible to operators, human oversight of many drones operating in combat must be reduced to the minimum necessary to prosecute the electronic warfare. Automated target acquisition will transfer initiative to the autonomous drone, and a robust, anti-jam communications network that protects against hostile jamming, capturing, and manipulation of data is a crucial enabler of drone swarming (DoD 2005).

Kallenborn (2018), from the U.S. National Defense University, defines 'drone swarm technology' as the ability of drones to autonomously make decisions based on shared information. This has the potential to revolutionize the dynamics of conflict. In fact, swarms will have significant applications to almost every area of national and homeland security. Swarms of drones could search the oceans for adversary submarines. Drones could disperse over large areas to identify and to eliminate hostile surface-to-air missiles and other air defenses. Drone swarms could potentially even serve as novel missile defences, by blocking incoming hypersonic missiles. On the homeland security front, security swarms equipped with chemical, biological, radiological, and nuclear (CBRN) detectors, facial recognition, anti-drone weapons, and other capabilities offer defences against a range of threats.

McMullan (2019) argues that swarming drones come in different shapes and sizes. For example,

the U.S. Defense Advanced Research Projects Agency (DARPA) has been working on a program dubbed Gremlins—micro-drones the size and shape of missiles—designed to be dropped from planes and to perform reconnaissance over vast areas. On the other side of the spectrum is the larger XQ-58 Valkyrie drone (8.8 m in length).

A San Diego company, Kratos Defense & Security Solutions produces two classes of jet-powered autonomous drones, the UTAP-22 Mako and the XQ-58 Valkyrie, which would collaborate with manned fighter jets as a 'loyal wingman' for a human pilot. They can carry precision-guided bombs and surveillance equipment (Gregg 2019b).

In 2016, DARPA launched the OFFensive Swarm-Enabled Tactics (OFFSET) program that envisions future small-unit infantry forces using swarms comprising upwards of 250 small Unmanned Aircraft Systems (UASs) and/or small Unmanned Ground Systems (UGSs) to accomplish diverse missions in complex urban environments. By leveraging and combining emerging technologies in swarm autonomy and human-swarm teaming, the program seeks to enable rapid development and deployment of breakthrough capabilities. OFFSET aims to provide the tools to quickly generate swarm tactics, to evaluate those swarm tactics for effectiveness, and to integrate the best swarm tactics into field operations. OFFSET will develop an active-swarm tactics-development ecosystem and supporting open-systems architecture, including

1) An advanced human-swarm interface to enable users to monitor and to direct, potentially, a real-time, networked virtual environment that would support a physics-based, swarm tactics game and
2) A community-driven swarm tactics exchange (Chung 2016).

OFFSET program, by leveraging and combining emerging technologies in swarm autonomy and human-swarm teaming, seeks to enable rapid development and deployment of breakthrough capabilities. The program consists of five research and experiment areas: swarm technology, human-swarm teaming, swarm perception, swarm networking, and swarm logistics. **Figure 1**, below, illustrates the autonomous swarm capability development of the OFFSETprogram (Peters 2019).

In August 2019, DARPA tested OFFSET by using a swarm of autonomous drones and ground robots to assist with military missions. DARPA showed how its robots analysed two city blocks to find, surround, and secure a mock city building (Peters 2019).

Finland's Ministry of Defense (Finland MoD 2015) addresses the reality that, in some cases, drones can carry out missions better and cheaper than manned aircraft. The widespread proliferation of Micro Air Vehicles (MAV), which are difficult to detect, is on the cusp of becoming extremely challenging for air defences. Even the smallest drones are suitable for intelligence and Precision Guided Munitions (PGM) for target designation. Moreover, they can double as weapons, even inside buildings. The most radical concepts focus on replacing the intelligence-targeting fire chain; they aim at achieving a rapid weapons effect with the coordinated use of swarming Unmanned Aerial Vehicles. This requires sufficient survivability and cost-effectiveness from drones to saturate the defence.

In an article presented at the *14th Annual International Conference on Cyber Warfare and Security*

(*ICCWS 2019*), Haberl and Huemer (2019) described the drone swarm attack. In 2018, the Russian Ministry of Defence announced that 13 drones, which had been fitted with small bombs, managed to attack Russian bases in Syria. Such drones, which are intended to explode on impact, need to be modified in order to carry explosives. It is easy to imagine how 3D-printing could come in handy in this regard, especially since drones are capable of evading missile warning systems without any additionally needed infrastructure or equipment.

As defined below, swarming is the coordinated use of various drones which might be of different types, 'intelligence', size, and capabilities so they can act in unison. This use of swarming techniques, where numerous drones are used for one purpose is of increasing interest. Generally, when dealing with security-related actions, there are two main emphases—overwhelming force and deception. The decreasing cost of smaller drones (Hambling 2015) plus the built-in redundancy of swarms make the use of many drones for an attack much more appealing as they tend to overwhelm any countermeasures against them. Also, it can make deception much more difficult for the number of drones, but some drones that are disabled will still leave others to carry out the mission. Thus, at its simplest, an attack of sacrificial, impact aerial drones in a swarm makes an effective tactic which can overwhelm the opponent.

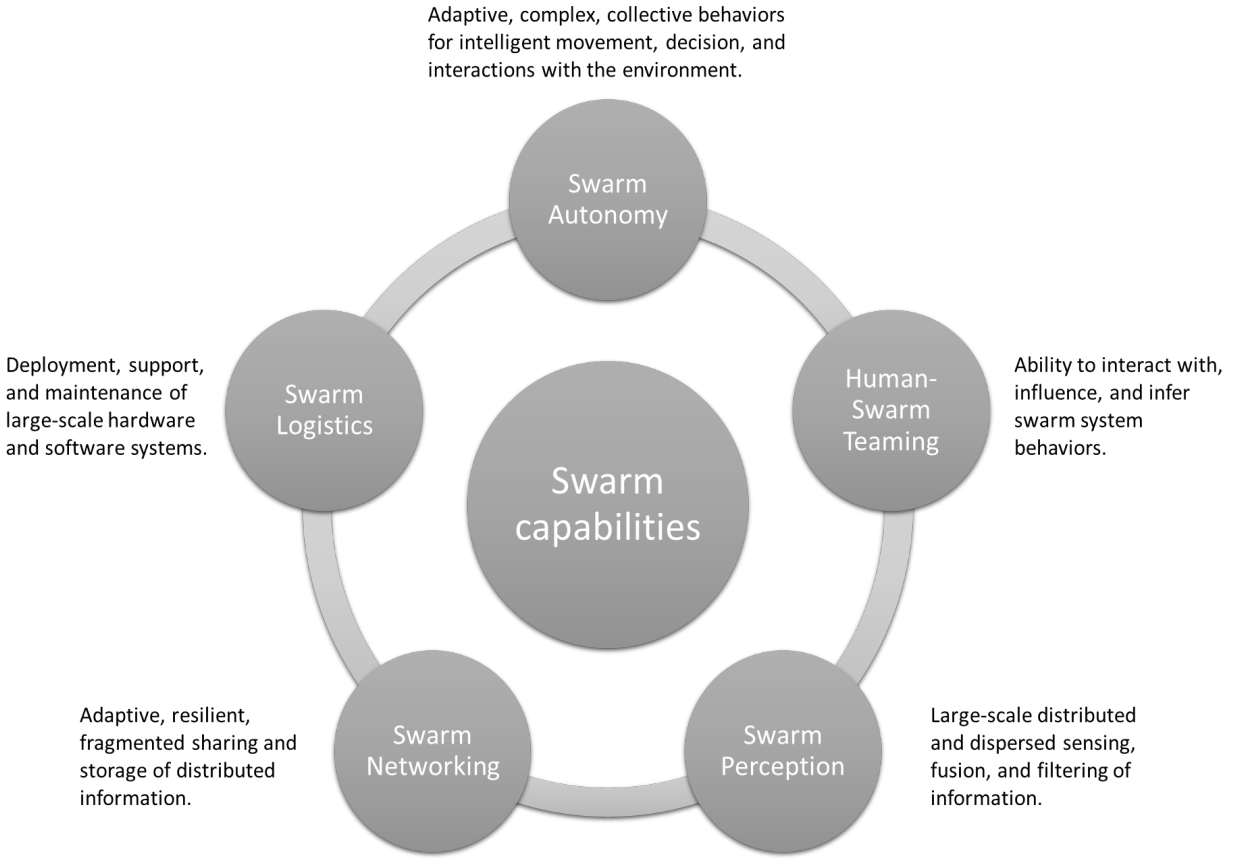

Figure 1: Autonomous swarm capability development in OFFSET program (modified from Chung 2016)

At present, these 'swarming drone systems' seem to be considered for underwater protection of valuable assets, such as submarines, and in the air for protecting manned aircraft, thus, providing surveillance for military units at a cheap cost. The initial use of 'tethered' drones linked to a

'mothership' gives protection to the controlling vehicle and its crew which, in turn, gives extra surveillance facilities and possibly firepower as well as cover by providing sacrificial drones to the central-control function. This concept develops into autonomous swarms, whereby each drone is independent but keeps communications with other drones and acts like one entity much like a flock of birds (Singer 2009). This implementation gives the group a lot more power and is much more difficult to deceive unless its elements are consistently very simple. However, simple, self-organizing swarms can lose some members without losing too much functionality, so deceiving and/or destroying the swarm will be harder than deceiving the individual. Nevertheless, swarms, because they need to link up with each other, are more vulnerable to infection from malware. Ironically, this vulnerability could be a weak point where software can be inserted.

Underwater drones do have a communication problem especially when not tethered to a 'mother ship' as communication signals are attenuated by the water medium. Signals are sent by radio and acoustic means or by light (blue has been used up to now). However, this has been partially overcome by using each drone arranged into a network of lines, passing the signal from one to another, and, thereby, extending the range much as classical network technology does.

The concept of swarms came out of a need to find asymmetric approaches to developing terrorist and insurgent approaches to war. From the U.S. perspective, the enemy in the early 21st century tended to be relatively small dispersed groups compared to conventional forces. Although these tactics were not new (Arquilla & Ronfeldt 2000), they did seem to be needed to compensate for the large, hierarchical forces which did not prove as flexible and speedy as these small groups. With the development and continuing advancement of military drones came the technological ability to produce smaller and more flexible varieties. As this development advanced, the increased communications and AI techniques allowed an ever-increasing potential of these machines to provide advanced drone swarms. The extension of network theory allowed the development of intelligent swarms which broadly can be hierarchical or networked (in an organizational sense).

Swarms can be designed so that the development of swarming systems can allow each element to work independently and come together in a swarm when needed so groups of drones can be expanded or decreased as the problem being tackled varies. Hence, drones of various abilities, functions, and forms can be coordinated, as necessary. This ability is very powerful and would require an opponent to work at a population level rather than targeting an individual drone. A well-chosen targeted drone might have the desired impact, but this would depend on the architecture of the network (Newman 2018).

To a large extent, a swarm is a mobile network with flexible architectures—as in a conventional network—but with a robot and sensors at the nodes and AI controlling the functionality and operations of the swarm itself and its objectives.

Issues with Mini-Drones

The proliferation of drones has raised a vast number of issues with their use, efficacy, ethical implications, control, and specific impacts on conflict. The following sections examine five of these issues.

Issue 1: The implications of mini-, micro- and nano-drone swarms

UAVs come in various sizes and have the ability to fly and hover, and range from the cheap Dragon

to more expensive Black Hornet. Many of these are designed around insect structures and can capture video from over a kilometer away. The lower-cost drones can be used in a swarm and, with the software constructed, combined with the sensor inputs could emulate the performance of the more expensive drones. The RoboBee is only three centimeters across and weighs 80 milligrams (Grossman 2018). These ultra-small drones are useful for covert surveillance as single entities (often over short distances) and can be flown inside buildings. In swarms, they can have the same effect but are more likely to be spotted. Whilst the engineering for these devices is well advanced, the real secret is the AI driving the swarm coordination and sensors. Hambling (2015) puts a large emphasis on the development of the software, using such techniques as neural networks to improve their performance. These swarms would be harder to spot and could deliver not only good intelligence, but targeted physical effects as well. Of course, these swarms can be used to inspect hazardous environments, such as nuclear accidents, bush fires, and marine environments, by, for example, carrying a line between vessels in stormy conditions. The larger ones can be used as a cheaper and more specific option to deliver materials, such as food, where people are isolated because of fires, avalanches, and epidemics. The micro- and nano-drones can also be used for inspection of injured victims.

Issue 2: Other types of drone swarms and their implications

Sanders (2017) classifies drone swarms into three categories:

- Aerial
- Ground
- Maritime

These categories can be further subdivided by Maritime (Surface), Maritime (Subsurface), and Space. In the aerial environment, Sanders (2017) uses Russia's six-generation fighter jet with five to ten unmanned drones to increase intelligence and targeting. These can leave the atmosphere. The U.S. and NATO have comparable capacity. Employing an example from the Chinese use of drones, Sanders (2017) states that functionality comes from decoying, jamming, and general electronic warfare, as well as kamikaze attacks. In other words, many nations are using them for multiple uses.

Sanders (2017) states that ground drones will be "ubiquitous, self-organized and collaborative". Of course, they can function without any rest. Most of these drones are larger than the mini- drones, discussed above. However, the concept and application of 'smart dust' which consists of wireless networked MicroElectromechanical Systems (MEMs) is comparable to that of a ground-based swarm (Marr 2018). These tiny, grain-sized devices can collect data on such things as moisture and sound, and can store it and/or send it back to a base.

In the maritime environment, various drone swarms have been developed for surface and amphibious craft as well as swarms for submarines that are analogous to those associated with fighter aircraft—that is, to collect intelligence around inshore areas and ports as well as data needed for the safety of the submarine mother ship. The UK has developed a fully functional Unmanned Underwater Vehicle (UUV) for the Royal Navy to act as a substitute for Hunter-Killer manned submarines (Jagger 2020).

Issue 3: Will the development of small drone swarms encourage the advancement changes in conflict tactics such as asymmetric war and terrorism?

As the development of state-based war often leads towards an asymmetric format, the distinctions between both the 'conventional' and civilian conflicts seem to be merging. The Russian use of Hybrid Warfare (Galeotti 2016), the Chinese use of the 'Unrestricted Warfare' doctrine (Liang & Xiangsui 2015) and the American doctrine of the Third Offset (Center for Strategic and International Studies [CSIS] 2017) have led to a situation that avoids major battles or outbreaks of violence. The methods of conflict seem to be moving to be more of an emphasis on 'softer' approaches, such as cyberwar, information warfare, and influence operations. These show similarities to counter-insurgency situations and, since 9/11, the militarization of law enforcement has increased. Korpela (2017) points out that demographic movements will encourage the growth of larger and heavily populated cites. This environment is conducive for the use of mini-drones for real-time surveillance for both low-level civil violence and the distribution of leaflets, and crowd control chemicals. Of course, the relative low cost of these functionally relevant drones encourages all sides to use them. This is aided by the general skills base in flying drones learned from electronic games and hobby drones as well as familiarity with software and hardware of these robots. In an asymmetric warfare scenario, mini-, micro-, and nano-drones have significant flexibility to provide surveillance, psychological, and kinetic functionality.

Issue 4: How will micro- and nano-drone swarms increase social surveillance?

The amount of surveillance of the public has increased significantly in recent times in various countries. As mentioned above, drones can be used by almost anyone to obtain legal and illegal data. The use of mini- and micro- drones by Chinese authorities for their Social Credit System (Kobie 2019) is well recorded. Although in the West the surveillance is not so oppressive, it is increasing in its coverage. Phenomena such as Smart Cities, traffic monitoring, and CCTV coverage provide, in some instances, an oppressive public environment. The Internet of Things (IoT) (Bhuvaneswari & Porkodi 2014) has certainly provided an interface between physical devices and the Internet. This provides a platform for surveillance. The coupling of drone swarms into the IoT has provided some detrimental effects as, in a sense, it is providing a conflict situation even when the stated aim is seemingly legitimate, such as monitoring traffic, high streets, or troublesome housing estates. In overt areas of conflict, swarming drones are known to have detrimental effects on its victims (as well as benefits for the owners of the system). Nemar (2017) describes the potential psychological distress caused by the constant surveillance as well as the potential for harm done by swarms of any size given the kinetic impact they can cause. While this might seem a far cry from some 'innocent' civilian networks of face-recognition cameras in local streets and network-linked devices that control such things as water flow in a reservoir, pouring molten metal in a smelter, a satellite-driven navigation device in a truck, or a remote-control initiator of a domestic heater, the potential to create havoc is still there. This is especially true as the IoT is not renowned for its security prowess (Etter 2016).

Issue 5: Will autonomy of drone swarms especially (LAWs) cause ethical dissonance?

This issue is debated continuously among those who see it as a development in a competitive arms race between various nations and other groups (for instance, Brock 2017) and those who prefer to challenge this on ethical grounds. Although a drone's capability is determined by its software/algorithms, its suite of sensors, and generally its automatic systems are used to control the machine by instructions from the AI driver. An autonomous drone would have the 'human-out-of-the-loop' scenario, where the drone itself would make independent choices about the target-and-

kill command. Normally, a human pilot would make the choice; or, if it was automatic, then the (supposedly) built-in instructions would limit the drone to the conditions for which it was designed. However, Artificial General Intelligence (AGI) is different because it assesses the situation from its sensors and can change the algorithms that control it by machine learning. Therefore, over time, the initial designers of the drones might not know what drives the conditions in which lethal force will be used. This is a dilemma as autonomous drones might be needed for very rapid responses. Is it an ethical activity in war to allow the decision of life and death to be made at the discretion of a machine?

A 2019 report to the U.S. Congress (Congressional Research Service 2019) has implied that AI will be used in many aspects of conflict: Intelligence, Surveillance, Reconnaissance, Information Operations, Cyber Operations, and Command and Control. There are some who are extremely optimistic about the future of these aspects, for example, Hambling (2015) who thinks the development of AI for drone swarms will increase exponentially as Moore's Law did with microprocessors. Others like Cross (2020) are a bit more reticent about the future abilities of drones to be used in conflict. Whatever the future of drones, Payne (2018) feels that they will be a significant factor in the future of conflict. Will the inner conflict between accidental killing and the efficiency of the drone swarm as a weapon cause any dissonance?

Conclusion

The concept of a swarm inherently drives drone development toward autonomy. Smart drone swarm technology could have a significant impact on every area of military capability, from enhancing supply chains to Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance and Reconnaissance (C5ISR) and delivering kinetic ammunitions. Swarms of small attack drones that confuse and overwhelm antiaircraft defence could soon become an important part of the modern military arsenal; and, as Britain's defence secretary has said, it is something that would "mark a major evolution in robot-enabled warfare" (Gregg 2019a).

The fact that the components of the swarm can communicate with one another makes the swarm different from a group of individual drones. Smart communication and autonomy allow the swarm to adjust behavior in response to real-time information. Drones equipped with cameras and other environmental sensors (sensor drones) can identify potential targets, environmental hazards, or defenses and can relay that information to the rest of the swarm. The swarm may then maneuver to avoid a hazard or defense, or a weapon-equipped drone (attack drone) may strike the target or defense. Real-time information collection makes drone swarms well-suited for searching over broad areas for mobile or other hard-to-find units in military or civilian operations.

While individual drones can be useful, a swarm of them would be more difficult to eliminate. A swarm of drones would help with a complicated environment, like an urban or covered terrain, where it is hard to see long distances. A large group of drones can provide better situational awareness than single drone.

According to Kallenborn (2018) a future drone swarm need not consist of the same type and size of drones but could incorporate both large and small drones equipped with different payloads. Joining a diverse set of drones creates a whole that is more capable than the individual parts. A single drone swarm could even operate across domains, with undersea and surface drones or ground and aerial drones coordinating their actions.

Swarming also adds new vulnerabilities. Drone swarms are particularly vulnerable to electronic warfare attacks. Because drone swarms are dependent on drone-to-drone communication, disrupting that signal also disrupts the swarm. As swarms become more sophisticated, they will also be more vulnerable to cyberattack. Adversaries may attempt to hijack the swarm by, for example, feeding it false information, hacking it, or generating manipulative environmental signals (Kallenborn & Bleek 2019)

How can an entity defend against a drone swarming attack? The US Air Force unveiled a new tool for that: a high-powered microwave system called Tactical High-Power Microwave Operational Responder (THOR), which is designed to protect bases against swarms of drones. According to the USAF, this system is designed to take out a large number of drones all at once and has a further range than bullets or nets (Cohen 2019). The counterattacks needed against small and very small drone swarms will need to be manifest as there are so many types and volumes of single drones present, as well as a multitude of configurations, sensors, physical environment of conflict, and swarm performance abilities to make it difficult to counter their missions. Of course, many of these swarms have much in common but they also have multiple structures and operational environments and aims and the ability to change their structures, sensors, and AI functions. It is unlikely to be an easy task to counter a well-structured swarm.

The variety of small drones combined with swarm configurations is enormous and, with such a flexible tool, applications are likely to be very diverse and to have an enormous impact on the practices used in conflict.

It is significant that on the first page on Wittes and Blum's (2016) text on the Future of Violence they paint a scenario of Do-It-Yourself (DYI) built drones to spread deadly spores over the country. Although drone swarms are not mentioned, the use of a swarm could be disastrous.

Drone Swarms are sophisticated combinations of hardware and software. They are almost universal in their potential benefits; however, this is true for their potential dangers as well.

References

Altigator Unmanned Systems 2019, viewed 3 Oct 2019, <https://altigator.com/drone-uav-uas-rpa-or-rpas/>.

Arquilla, J & Ronfeldt, D 2000, *Swarming and the future of conflict*, RAND, Santa Monica, CA, US.

Bhuvaneswari, V & Porkodi, R 2014, 'The Internet of Things (IoT) applications and communication enabling technology standards: An overview, *Proceedings of the 2014 International Conference on Intelligent Computing Applications*, Coimbatore, Tamil Nadu, IN, viewed 20 June 2019, pp. 324-9, <http://ieeexplore.ieee.org/abstract/document/6965065>, doi: 10.1109/ICICA.2014.73.

Brock, JW 2017, *Why the United States must adopt lethal autonomous weapons systems*, United States Army Command and General Staff College, Fort Leavenworth, KS, US.

Chung T 2016, 'OFFensive Swarm-Enabled Tactics (OFFSET)', viewed 5 October 2019, <https://www.darpa.mil/program/offensive-swarm-enabled-tactics>.

Cohen RS 2019, 'Microwave weapons moving toward operational use', *Air Force Magazine*, 20 March, viewed 15 October 2019, <https://www.airforcemag.com/microwave-weapons-moving-toward-operational-use/>.

Congressional Research Service 2019, *Artificial Intelligence and national security*, updated 21 November 2019, Washington DC, US.

Cross, T 2020, 'Reality check', *The Economist Technical Quarterly*, 13 June, pp.3-4.

Center for Strategic and International Studies (CSIS) 2017, *Assessing the Third Offset Strategy*, Center for Strategic and International Studies, March, Washington, DC, US.

Department of Defense (DoD) 2005, *Unmanned Aircraft Systems roadmap 2005-2030*, Office of the Secretary of Defense, 20 July, Pentagon, Arlington, VA, US.

——2014, *Unmanned Systems Integrated Roadmap 2013-2038,* Under Secretary of Defense Acquisition, Technology & Logistics, January, Pentagon, Arlington, VA, US.

——2018, *Unmanned Systems Integrated Roadmap 2017-2042*, Office of the Secretary of Defense, 28 August, Pentagon, Arlington, VA, US.

Etter, D 2016, *IoT Security: Practical guide book*, Lightning Source, Milton Keynes, UK.
Finland Ministry of Defence (MoD) 2015, *Preliminary assessment for replacing the capabilities of the Hornet Fleet final report*, Ministry of Defence, 08 June, Helsinki, FI.

Galeotti, M 2016, *Hybrid War or Gibridnaya Voina? Getting Russia's non-linear military challenge right*, Mayak Intelligence, Milton Keynes, UK.

George, P 2019, 'Artificial intelligence system 'too good' to be released but drone development continues', Your NZ, 20 February, viewed 21 September 2020, <https://yournz.org/2019/02/20/artificial-intelligence-system-too-good-to-be-released-but-drone-development-continues/>.

Gregg A 2019a, 'A key U.S. ally is close to adding swarming attack drones to its military arsenal', *Washington Post*, 15 February, viewed 21 September 2020, <https://www.washingtonpost.com/business/2019/02/15/key-us-ally-is-close-adding-swarming-attack-drones-its-military-arsenal/>.

——2019b, 'Swarming attack drones could soon be real weapons for the military', *Washington Post*, 19 February, viewed 5 October 2019, <https://www.latimes.com/business/la-fi-drone-swarms-20190219-story.html>.

Grossman, N 2018, *Drones and terrorism: Asymmetric warfare and the threat to global security*, Taurus and Co., London, UK.

Haberl F & Huemer F 2019, 'The terrorist/*jihadi* use of 3D-printing technologies: Operational realities, technical capabilities, intentions and the risk of psychological operations', *Proceedings of the 14th Annual International Conference on Cyber Warfare and Security* (*ICCWS 2019*), 28 February-1 March 2019, Stellenbosch, ZA.

Hambling, D 2015 *Swarm troopers*, Archangel Ink. Venice, FL, US.

International Civil Aviation Organization (ICAO) 2019, *Remotely Piloted Aircraft System (RPAS) Concept of Operations (CONOPS) for international IFR operations*, viewed 11 October 2019, <https://www.icao.int/safety/UA/Documents/ICAO%20RPAS%20CONOPS.pdf>).

Jagger,S 2020, 'Royal Navy to field large "robot subs"', *Warships International Fleet Review*, p 34.

Joint Air Power Competence Centre (JAPCC) 2014, 'Remotely Piloted Aircraft Systems in contested environments: A vulnerability analysis', September, viewed 12 October 2019, <https://www.japcc.org/portfolio/remotely-piloted-aircraft-systems-in-contested-environments-a-vulnerability-analysis/>.

Kallenborn Z 2018, *The era of the drone swarm is coming, and we need to be ready for it*, Modern War Institute at West Point, 25 October, viewed 17 October 2019, <https://mwi.usma.edu/era-drone-swarm-coming-need-ready/>.

——& Bleek PC 2019, 'Drones of mass destruction: Drone swarms and the future of nuclear, chemical, and biological weapons', *The Nonproliferation Review*, vol. 25, nos. 5-6, Special section on the nuclear dimensions of the 1967 Arab–Israeli War, pp. 523-43, 2 January, viewed 2 January 2019, <https://doi.org/10.1080/10736700.2018.1546902>.

Kobie, N 2019, 'The complicated truth about China's social credit system', *Wired*, viewed 8 July 2020, <https://www.wired.co.uk/article/china-social-credit-system-explained>.

Korpela, C 2017, 'Swarms in the Third Offset', ed. White, S.R, *Closer than you think: The implications of the Third Offset Strategy for the U.S. Army*, US Army Command and General Staff College, Fort Leavenworth, KS, US.
Liang, Q & Xiangsui, W 2015, *Unrestricted warfare: China's master plan to destroy America,* Echo Point Books & Media, New York, NY, US.

Marr, B 2018, 'Smart dust is coming. Are you ready?', *Forbes,* viewed 8 July 2020, <https://www.forbes.com/sites/bernardmarr/2018/09/16/smart-dust-is-coming-are-you-ready/#4b099ec05e41>.

McMullan T 2019, 'How swarming drones will change warfare', BBC News, 16 March, viewed 15 October 2019, <https://www.bbc.com/news/technology-47555588>.

Nemar, R 2017, 'Psychological harm', *The Humanitarian impact of drones*, eds. R Acheson, W Bolton, E Minor & A Pytlak, Women's International League for Peace and Freedom, International Disarmament Institute, New York, NY, US, pp. 36-47.

Newman, M 2018, *Networks,* 2nd edn., Oxford University Press, Oxford, UK.

Papireddy, T 2015, *Tracking and monitoring Unmanned Aircraft Systems activities with crowd-based mobile apps*, 1 May, School of Computer Science, Howard R. Hughes College of Engineering, University of Nevada, Las Vegas, NV, US.

Payne, T 2017, 'Lethal autonomy: What it tells us about modern warfare', *Air & Space Power Journal*, vol. 15, no. 14, Winter, pp. 16-33.

——2018, *Strategy, Evolution, and War*, Georgetown University Press, Washington, DC, US.

Peters, J 2019, 'Watch DARPA test out a swarm of drones', *The Verge*, 9 August, viewed 18 October 2019, <https://www.theverge.com/2019/8/9/20799148/darpa-drones-robots-swarm-military-test>.

Pritchard S 2019, 'Drones are quickly becoming a cybersecurity nightmare', *Threatpost,* vol. 22, March, viewed 15 October, <https://threatpost.com/drones-breach-cyberdefenses/143075/>.

Pennsylvania State University 2019, 'Classification of the Unmanned Aerial Systems', University Park, PA, US, viewed 12 October 2019, <https://www.e-education.psu.edu/geog892/node/5>.

PricewaterhouseCoopers (PwC) 2016, 'Global market for commercial applications of drone technology valued at over $127bn', *PwC blog*, 9 May, viewed 11 October 2019, <https://pwc.blogs.com/press_room/2016/05/global-market-for-commercial-applications-of-drone-technology-valued-at-over-127bn.html>.

Sanders, AW 2017, *Drone swarms*, School of Advanced Military Studies, Fort Leavenworth, KS, US.

Singer PW 2009, *Wired for war: The robotics revolution and conflict in the 21st century*. Penguin Books, London, UK.

Single European Sky ATM Research (SESAR) 2016, European Drones - Outlook Study -Unlocking the value for Europe, 1 November, European Union and Eurocontrol, Brussels, BE.

Wittes, B & Blum, G 2016, *The future of violence: Robots and germs, hackers and drones*, Amberley, Stroud, UK.