Mini-Drones Swarms and Their Potential in Conflict Situations

Martti Lehto[1] and Bill Hutchinson[2]
[1]University of Jyväskylä, Finland
[2]Edith Cowan University, Australia
martti.j.lehto@jyu.fi
w.hutchinson@ecu.edu.au
DOI: 10.34190/ICCWS.20.084

Abstract: The Unmanned Aerial Vehicles (UAV) commonly known as drones are currently used in a wide range of operations such as border monitoring, aerial reconnaissance, traffic control and military interventions in armed conflicts. These aerial vehicles are expected to be reliable, automated and sometimes autonomous machines, albeit the human factor continues to play a crucial role in programming and control. At their genesis, drones were complex, large and reserved to an exclusive club of technologically advanced military powers. They tended to be used against technologically weak military targets. Developments in the price, size and sophistication of drones has now enabled almost anyone to purchase them. These contemporary machines are often small, and, with increasing usage of Artificial Intelligence (AI) has put them in the cost and usage range of almost any combatant. Therefore, there is a need to re-think strategies and tactics for their use. These 'mini-drones' rarely have the sophistication and capabilities of 'conventional' drones, but they do have the ability to provide an asset in large numbers and increasing capabilities. Although they might not have such attributes as the lifting capabilities of the larger models, they can be used economically and en masse and so have can have a different but equally effective outcomes. 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. Thus, sophisticated AI provides a swarm with various types of functionality to the drones: for instance, dummy/distraction drones, kinetic and non-kinetic attack drones, surveillance drones as well as drones that can be equipped with wireless access points and deployed to configure an ad-hoc flying network. This paper also examines UAV/drone categories and autonomy and also how autonomy and Swarm intelligence (SI) can be used to create efficiency for a variety of operation concepts.

Keywords: drone, security, artificial intelligence, swarming

1. Introduction

There is no one standard when it comes to the classification of unmanned aircraft system (UAS) sometimes called an Unmanned Aerial Vehicle (UAV). Defense agencies have their own standards, 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. An UAS is a "system whose components include the necessary equipment, network, and personnel to control an unmanned aircraft." In some cases, the UAS includes a launching element. (DoD, 2014)

An Unmanned Aircraft is defined as a powerful system, that does not carry a human operator, uses aerodynamic forces to provide vehicle lift, can fly autonomously or be piloted remotely; it can be expendable or recoverable, and can carry a payload. (Papireddy, 2015)

The International Civil Aviation Organization (ICAO) employs the acronym RPAS (standing for Remotely Piloted Aircraft System). The definition is: "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)
By being 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 unmanned aerial vehicles as drones. In a general way, many countries use the term 'drone'. For many, UAVs are mostly used in a military context. However, drones cover both civil and military purposes of any type of aerial unmanned vehicle. (Alligator Unmanned Systems, 2019)

This article uses the term drone to cover the whole spectrum of unmanned aerial vehicles. The research focuses on categories, autonomy, military and civilian operations, and swarming. The study has used content analysis as a research method drawing analysis from various documents. The resulting data collected are summarized in order to provide better understanding of both advantages and inconveniences associated with development and wide utilization of drones in a variety of settings.

2. Drone categories and autonomy

2.1 Drone categories

There is no one standard when it comes to the classification of unmanned aircraft system (UAS). Defense agencies have their own standards, and civilians have their own categories. Unmanned aircraft can be roughly divided into fixed winged and rotary winged. Multi-rotor helicopters are referred to as multi-copters. Other classification arguments are: size, Maximum Gross Takeoff Weight (MGTW), range and endurance. For combat, there are two main groups: Unmanned Combat Aerial Vehicle (UCAV) and Unmanned Combat Aerial Rotorcraft (UCAR). 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. According to the U.S. Department of Defense (DoD2), as illustrated in Tables 1 &2 below, the commonly used ones include:

- 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, the motors are arranged in pairs on top of each other)

Table 1: UAVs Classification according to the US Department of Defense (DoD) (PSU, 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 2: UAVs Classification according range and operating time (PSU, 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

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

Table 3: UAV classification-based capability

UAV	Capability
Micro Unmanned Aerial Vehicle (MUAV)	Producing information within a radius of less than 100 kilometers from its land station.
Tactical Unmanned Aerial Vehicle (TUAV)	Producing information within a radius of about 200 kilometers of its land station.
Medium Altitude Endurance Unmanned Aerial Vehicle (MAE)	Producing information within a radius of about 750 kilo meters 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.

Over the past two decades, Remotely Piloted Aircraft System(s) (RPAS) 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 to Reconnaissance RPAS, which are expected to be upgraded and continue the role of current medium-altitude long-endurance (MALE)/ High-Altitude Long Endurance (HALE) systems, is illustrated in Table 4 below. (JAPCC, 2014)

Table 4: UCAV classification based on combat missions

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 maneuverability	Designated to conduct air-to-air and air to-ground combat in non-permissive and hos-tile 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, designated to project military power like naval aircraft carriers

2.2 Drone autonomy

Autonomy allows for the reduction of the frequency at which the operators must interact with the drone and supporting the implementation of more robust system solutions, where the role of the operators is to manage and 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 centered on ethically relevant subprocesses of the system as a whole; targeting, goal-seeking, and the initiation of lethality (Payne, 2017).

According US 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 automated systems, which are governed by prescriptive rules that allow for no deviations. While early robots generally only exhibited automated capabilities, advances in Artificial Intelligence and Machine Learning (ML) technology allow 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 near fully autonomy. The following autonomous categories have been identified:

Semiautonomous (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.

Supervised Autonomous (Human-on-the-loop): The AI controls all aspects of its operations, but humans monitor the operations and can intervene when, and if, necessary.

Fully Autonomous (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 automated, but they are not autonomous. US Office of the Under Secretary of Defense (2016) addresses 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.

3. Drone's military and civilian operations

3.1 Drone's military operations

The development of unmanned aerial vehicles is intensifying as related technologies are becoming cheaper. Drones can be used in a flexible manner in performing different 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 (EW), Combat Search and Rescue (CSAR) operations, Chemical, Biological, Radiological and Nuclear Warfare (CBRN) threats motoring, payloads and

logistics transportation. Even in deploying Counter Improvised Explosive Devices (C-IED) in areas where the risk level is too high for human interventions.

Drones are presumed to provide their services at any time, be reliable, automated and autonomous. Based on these presumptions, governmental and military leaders expect drones to improve national security through surveillance 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 enclosed make drones an extremely interesting target for espionage and exposed these versatile aerial vehicles to 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 deny enemy movements and maneuvering. Unmanned combat aircraft can be divided into two categories according to their operating model: loitering or swarming.

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.

3.2 Drone's civilian operations

Various UAVs are increasingly being used for various civilian purposes, such as government missions (e.g., for law enforcement, border security, coastguard) or broader security and safety missions to include firefighting, surveillance of oil and gas industry infrastructure and electricity grids/ distribution networks, traffic control, disaster management, agriculture, forestry and fisheries, earth observation and remote sensing and communications and broadcasting.

According to Single European Sky ATM Research (SESAR, 2016) the growing drone marketplace shows significant potential, with European demand exceeding over 10 billion EUR annually, in nominal terms, by 2035 and over 15 billion EUR annually by 2050. Fortune Business Insights (2019) estimates that UAV market to Reach USD 27.40 billion by 2026.

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. In aggregate, some seven (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 in 2050. (SESAR, 2016)

Critical infrastructure (CI) includes large variety elements from nuclear reactors, chemical facilities, water systems, logistics and airports to healthcare and communications. Today drones play an important role in monitoring, maintaining and ensuring the safety and security of critical infrastructures. For example in the energy sector, drones are expected to improve maintenance and be used for inspections, which are segmented into two primary mission types: 1) local site inspections, performed by multi-copters operating today in Visual Line of Sight (VLOS) and below 150 meters altitude and 2) long range utility inspections for which the fleet is expected to be composed of Beyond Visual Line of Sight (BVLOS) fixed wing drones flying near 150 meters of altitude with potentially (SESAR, 2016). So, 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 cyber-attacks, causing disruptions or even 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, necessitating new actions to defend CI assets. Today some drones have payload capacity, extended range, and the ability to be GPS- or pilot-guided to locations with great precision. (Palmer & Geis, 2017)

Meanwhile, as there is a development from Cold War to "Code" War, highly trained cyber warriors continue to target defense and other protected computer information networks — thereby threatening critical infrastructures. For instance, built on and remotely guided by "codes," military drones are essentially versatile "flying computers" with the devastating power to hunt and kill the enemy. (Hyacinthe, 2009)

4. 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, ground and space for that matter) for extended periods and deny enemy movements and maneuvering. Unmanned combat aircraft can be divided into two categories according to their operating model: loitering or swarming.

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)

As widely documented, a loitering munition 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.

The widespread use of drones around the world is evident, 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 and security. 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 has increasing interest. A swarm could support lower operating costs, greater system efficiency as well as increased resilience in many areas. (Hutchinson, 2018)

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 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 US 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 or disperse over large areas to identify and eliminate hostile surface-to-air missiles and other air defenses. Drone swarms could potentially even serve as novel missile defenses, 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 defenses against a range of threats. Also, they could be used in attack mode as vectors of some of these scenarios.

McMullan (2019) argues that swarming drones come in different shapes and sizes. For example, the US 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 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 are able to carry precision-guided bombs and surveillance equipment. (Gregg, 2019)

DARPA launched in 2016 OFFSET-program (OFFensive Swarm-Enabled Tactics) 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, evaluate those swarm tactics for effectiveness, and integrate the best swarm tactics into field operations. OFFSET will develop an active swarm tactics development ecosystem and supporting open systems architecture, including:

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

At present, the flight path, sensor payload and weapons systems of airborne drones are coordinated from ground control stations. However, the concept of an autonomous or semi-autonomous wingman is arriving even faster than expected. Future fighters will be able to provide a drone with tasks and objectives, manage sensor payload and direct flight-path from the air. (Osborn, 2019)

In the OFFSET-program 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. The program consists five research and experiment areas: swarm technology, human-swarm teaming, swarm perception, swarm networking, and swarm logistics. Figure 1 illustrates the autonomous swarm capability development OFFSET-program. (Peters, 2019)

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

Finland’s MoD (2015) addresses 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) 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 in order to saturate the defence.

Haberl and Huemer (2019) described in their conference paper 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 and 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.

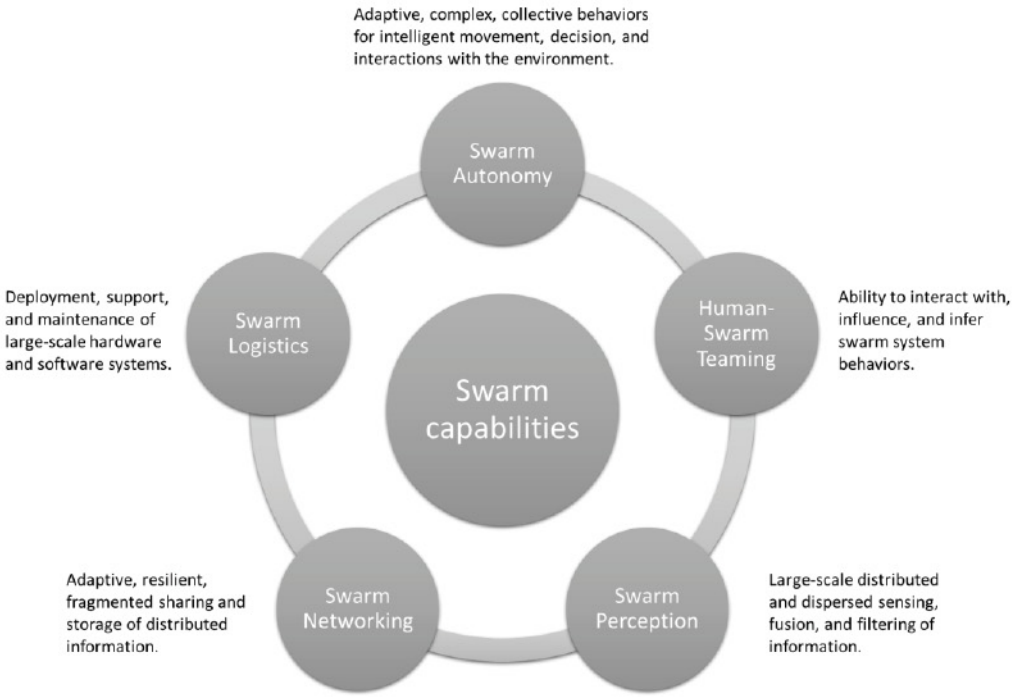

Figure 1: Autonomous Swarm Capability development in OFFSET-program (modified from Chung, 2016)

In swarming operations interconnected, co-operative drones are capable of working together intelligent. Swarm intelligence is the collective behavior of decentralized, self-organized systems, natural or artificial (Beni & Wang, 1993). This use of swarming techniques where numerous drones are used for one purpose is of increasing interest. Generally, when dealing with security related actins there are two main emphases - overwhelming force and deception. The decreasing cost of smaller drones (Hambling, 2015) plus the built-in redundancy of swarms makes the use of many drones for an attack much more appealing as it tends to overwhelm any countermeasures against them. Also, it can make deception much more difficult as some drones that are disabled will still leave others to carry out the mission. Thus, at its simplest attack of sacrificial, impact aerial drones in a swarm makes an effective tactic which can overwhelm the opponent.

At present, these 'swarming drone systems' are used and considered for underwater protection of valuable assets such as submarines and in the air for protecting manned aircraft, 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 fire-power 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 acted 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 – 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 and ironically this could be a weak point.

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 being arranged into lines and passing the signal from one to another 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 US perspective, the enemy in the early 21st century tended to be relatively small dispersed groups compared to conventional forces. Although these tactics were not really new (Arquilla and 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 of military drones, and with the continuing advancement of them, 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 to develop 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 such 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, function and form, 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 (although a well-chosen targeted drone might have the desired impact, but this would depend on the architecture of the network). (Newman, 2018).

5. Conclusion and Discussion

The swarm idea inherently drives drone development toward autonomy. Smart drone swarm technology could have a significant impact on every area of military capability, for enhancing supply chains to C5ISR and delivering kinetic ammunitions. Swarms of small attack drones that confuse and overwhelm antiaircraft defenses could soon become an important part of the modern military arsenal, something that would mark a major evolution in robot-enabled warfare. (Gregg, 2019)

Advances in computer power, processing speed and AI are rapidly changing the scope of what platforms are able to perform without needing human intervention. At the moment, multiple humans are often needed to control a single drone, and new algorithms increasing autonomy for drones could greatly change this ratio. (Osborn, 2019)

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 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 for someone 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 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 domain, with undersea and surface drones or ground and aerial drones coordinating their actions. As established above, information dominance is reserved to wary military planners with the foresight to embrace system-of-systems landscape for warfare, in which networks of manned and unmanned platforms, weapons, sensors and electronic warfare systems interact each other (Birkey et.al, 2018).

Among other drawbacks, it is important to acknowledge that 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 cyber-attack. Adversaries may attempt to hijack the swarm by, for example, feeding it false information, hacking, or generating manipulative environmental signals. (Kallenborn and Bleek, 2019)

The international intelligence community has been on notice since the late 1930's. The scale might be all that has been modified from a 1944 German design of an unmanned aerial vehicle (UAV) intended to disperse

deadly airborne bioactive substances — according to U.S. intelligence accounts declassified by Los Alamos labs (Hyacinthe, 2009).

How to defend against drone swarming attack? US Air Force recently 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 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)

References

Alligator Unmanned Systems (2019) https://altigator.com/drone-uav-uas-rpa-or-rpas/, October 18, 2019.

Arquilla, J. & Ronfeldt, D. (2000) *Swarming and the Future of Conflict*, RAND, Santa Monica, CA.

Beni, G., Wang, J. (1993). *Swarm Intelligence in Cellular Robotic Systems*. Proceed. NATO Advanced Workshop on Robots and Biological Systems, Tuscany, Italy, June 26–30, pp. 703–712

Birkey D., Deptula D. Stutzriem L. (2018) *Manned-Unmanned Aircraft Teaming: Taking Combat Airpower to the Next Level*, Mitchell Institute Policy Papers, Vol. 15, July 2018.

Chung T. (2016) *OFFensive Swarm-Enabled Tactics (OFFSET)*, https://www.darpa.mil/program/offensive-swarm-enabled-tactics.

Cohen R. S. (2019) *Microwave Weapons Moving Toward Operational Use*, Air Force Magazine, March 20, 2019.

DoD (2005) *Unmanned Aircraft Systems Roadmap 2005-2030*, July 20, 2005.

DoD (2014) *Unmanned Systems Integrated Roadmap 2013-2038*, January 2014.

DoD (2018) *Unmanned Systems Integrated Roadmap 2017-2042*, August 28, 2018.

Fortune Business Insights. (2019) *Unmanned Aerial Vehicle (UAV) Market to Reach USD 27.40 Billion by 2026; Increasing Demand from Defense Forces to Boost Growth*, November 11, 2019 https://www.globenewswire.com/news-release/2019/11/11/1944568/0/en/Unmanned-Aerial-Vehicle-UAV-Market-to-Reach-USD-27-40-Billion-by-2026-Increasing-Demand-from-Defense-Forces-to-Boost-Growth-Fortune-Business-Insights.html

Gregg A. (2019) *Swarming attack drones could soon be real weapons for the military*, Washington Post, February 19, 2019.

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 ICCWS 2019, 28 February - 1 March 2019, Stellenbosch, South-Africa.

Hambling, D. (2015). *Swarm Troopers - How Small Drones Will Conquer the World*, Archangel Ink. Venice, USA.

Hutchinson W. (2018) *Deceiving Autonomous Drones: Some Implications?* Conference Proceedings of 17th Australian Cyber Warfare Conference (CWAR), October 10-11th, 2018, Melbourne, Victoria, Australia, pp. 55-67.

Hyacinthe B. (2009) *Cyber Warriors at War: National Security Secrets and Fears Revealed*. *Cyber Warriors at War: U.S. National Security Secrets and Fear Revealed* (2009). Xlibris, Indiana, U.S.A.

ICAO. (2019) *Remotely piloted aircraft system (RPAS) concept of operations (CONOPS) for international IFR operations.*

JAPCC. (2014) *Remotely Piloted Aircraft Systems in Contested Environments A Vulnerability Analysis*, September 2014.

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, October 25, 2018.

Kallenborn Z. and Bleek P. C. (2019) *Drones of Mass Destruction: Drone Swarms and the Future of Nuclear, Chemical, And Biological Weapons*, blog in War on the Rocks, February 14, 2019.

McMullan T. (2019) *How swarming drones will change warfare*, BBC News, March 16, 2019.

MoD. (2015) *Preliminary Assessment for Replacing the Capabilities of the Hornet Fleet*, Final Report, 8.6.2015.

Newman M. (2018) *Networks - second edition*, Oxford University Press, Oxford, UK.

Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (2016) *Report of the Defense Science Board Summer Study on Autonomy*, Washington, D.C., June 2016.

Osborn K. (2019) *The Air Force Is Testing A Secret Weapon: Drone Swarms*, The National Interest blog, October 10, 2019.

Palmer T. S., Geis II J. P. (2017) *Defeating Small Civilian Unmanned Aerial Systems to Maintain Air Superiority*, Air & Space Power Journal, Summer 2017.

Papireddy T. (2015) *Tracking and Monitoring Unmanned Aircraft Systems Activities with Crowd-Based Mobile Apps*, University of Nevada, USA, 1 May 2015.

Payne T. (2017) *Lethal Autonomy What It Tells Us About Modern Warfare*, Air & Space Power Journal, Winter 2017.

Peters J. (2019) *Watch DARPA test out a swarm of drones*, The Verge, August 9, 2019.

PSU. (2019) *Classification of the Unmanned Aerial Systems*, Pennsylvania State University, https://www.e-education.psu.edu/geog892/node/5.

SESAR. (2016) *European Drones - Outlook Study -Unlocking the value for Europe*, November 2016.

Ion A. Iftimie is an Eisenhower Fellow at the NATO Defense College in Rome. Formerly, he served as a Senior Cyber Planner at the United States Cyber Command. He is a graduate of the Harvard Kennedy School Executive Program in Cybersecurity Policies and of the Swedish Defense University Senior Course on Security Policy.

Abdul Bashiru Jibril is a PhD Candidate at the Faculty of Management and Economics, Tomas Bata University in Zlin, Czech Republic. He received his MSc. in Management and Marketing from the same University in 2018. He is a senior research assistant and a team leader of a Faculty-wide project. His main research areas are internet marketing, consumer behavior, and brand management.

Mr. Abiud Jimenez is a principal electrical engineer at Dynetics, Inc. He received his Master in Systems Engineering from SMU in 2006 and his BSEE from UTRGV. His main research involves studying effects on wireless communications systems caused by intended and unintended interference from electromagnetic waves.

Dr Keith Joiner joined the Air Force in 1985 and became an aeronautical engineer, project manager and teacher over a 30 year career before joining the UNSW in 2015 as a senior lecturer in test and evaluation. His expertise includes Defence Test and Evaluation of complex systems and platforms, their acquisition, design acceptance and operational acceptance, including to varying extents land, maritime, aerospace and joint systems and platforms.

Jennyphar Kahimise is a Master of Computer Science student at the Namibia University of Science and Technology (NUST). Her research interests includes Human Computer Interaction, Children safety online and cybersecurity.

Omer Faruk Keskin is a Ph.D. Student in Engineering Management and a Graduate Assistant in Old Dominion University. He holds an MS Degree in engineering management and a BS degree in systems engineering. His research is focused on risk and reliability analysis of critical infrastructure cyber physical systems.

Minchul Kim is a researcher of Agency for Defense Development, South Korea. He is currently in an integrated PhD program in Korea University. His main research areas are integrated cyber situational awareness system and algorithmic optimization.

Mr. Neal Kushwaha is the founder and CEO of IMPENDO Inc, a cyber security and data centre consulting firm in Canada. Annually, he hosts a conference in Ottawa, Canada called DCAR. During his spare time, he climbs big mountains in the Himalayas. Neal is also a recipient of the Silver Medal of Bravery.

Dr Michael Adu Kwarteng is an Assistant professor of Marketing and Management at Tomas Bata University in Zlin, Czech Republic. He received his PhD in Marketing from Tomas Bata University in 2018. His research interest is primarily centred on the application of internet in marketing and currently researching on online buying behaviour of customers in both developed and developing economies

Maxime Lagrasse is a French student from the Bordeaux Institute of Technology (Bordeaux-INP) working towards a five-year engineering degree, in the form of a special curriculum, with half-time lecture attendance and half-time work in a company as a system and network administrator.

Mr. Hyong Lee is a Senior Policy Analyst with NDU's Center for Applied Strategic Learning. His career includes being a Presidential Management Intern with the Army Cost and Economic Analysis Center and Chief, Decision Support Branch at US Pacific Command. He joined NDU in 2002 and provides gaming support to the College of Information and Cyberspace.

Dr. Martti Lehto, (Military Sciences), Col (GS) (ret.) works as a Professor (Cyber security) in the University of Jyväskylä. He has over 40 years' experience in C4ISR Systems in Finnish Defence Forces. Now he is a Cyber security and Cyber defence researcher and teacher and the pedagogical director of the Security and Strategic Analysis MSc. program. He is also Adjunct professor in National Defence University in Air and Cyber Warfare. He has over 140 publications on the areas of C4ISR systems, cyber security and defence, information warfare, artificial intelligence, air power and defence policy.