

# Threat of swarm of drones delivering weaponized explosives becomes real, DARPA seeks swarm protection technologies

The militant organizations have started employing drones to further their terrorism. The small drones such as a quadcopter or model airplane are readily available and they are increasingly used by terrorists to retrofit them, giving the aircraft the ability to deliver weaponized explosives or hazardous materials. In their hands, drones could, fly IEDs through the air to a target, or disperse a biological or chemical agent while its pilot remains safely distanced from contamination. The lethality of these drones can be further enhanced by operating them in Swarms.

The Russian Ministry of Defence claims its forces in Syria were attacked a week ago by a swarm of home-made drones – the first time such a coordinated assault has been reported in a military action. According to the Ministry of Defence, Russian forces at the Khmeimim air base and Tartus naval facility “successfully warded off a terrorist attack with massive application of unmanned aerial vehicles (UAVs)” last Friday night.

“As evening fell, the Russia air defence forces detected 13 unidentified small-size air targets at a significant distance approaching the Russian military bases,” the Ministry said in a statement. “Ten assault drones were approaching the Khmeimim air base, and another three – the CSS point in Tartus.” Six of the assault force drones were intercepted by Russian electronic warfare units, with three of the UAVs being brought

to land outside the base, while the remaining three exploded on contact with the ground. Another seven drones were “eliminated” by Pantsir-S anti-aircraft missiles fired by the Russians, with the bases reporting no casualties or damage, the statement explains.

Officials of the U.S. Defense Advanced Research Projects Agency (DARPA) in Arlington, Va., have released an industry solicitation for the Mobile Force Protection (MFP) program. The potential \$63 million project seeks ways to defend against not only today’s radio-controlled and GPS-guided weaponized UAVs, but also against future UAVs that navigate by visual means in large groups to gather intelligence and coordinate attacks against one or more high-value moving targets.

“The rapid evolution of small unmanned air systems (sUAS) technologies is fueling the exponential growth of the commercial drone sector, creating new asymmetric threats for warfighters. sUASs’ size and low cost enable novel concepts of employment that present challenges to current defense systems. These emerging irregular systems and concepts of operations in diverse environments require technology advancements to quickly detect, identify, track, and neutralize sUASs while mitigating collateral damage and providing flexibility to operations in multiple mission environments,” says DARPA.

## **Rapid advancement of Swarm technology**

UAV Swarms is emerging enabling technology that can find, fix, and communicate precise target location of ground, sea, and air targets; they can serve as weapons platforms to attack air defense systems from multiple axes; or they can pass missile targeting data to any platform carrying a counter air missile.

Advanced Robotic Systems Engineering Laboratory (ARSENL), a team of students at the Naval Postgraduate School in Monterey,

California, successfully launched a swarm of 50 drones, all of them being controlled by a single operator. The long-term goal is to have the swarms determine how to act on their own, and ARSENL reportedly intends to test this by eventually having a 50 vs. 50 drone swarm dogfight.

Swarm of drones are also being considered by military for future A2/AD environment. Future wars will be fought with swarms of expendable, disaggregated, intelligent systems rather than the big, expensive weapon platforms the U.S. has relied on for fifty years, said William Roper, the lead of the Pentagon's semi-secret Strategic Capabilities Office (SCO), adding that he believes the Air Force will have a greater challenge adjusting to this new reality than the other services. The end goal, in Roper's mind, is to limit the danger to individual operators. Rather than send in a wave of manned planes for the first day of combat, the SCO head said, send in wave after wave of cheap, disposable systems that come with no risk of losing a U.S. service member.

The U.S. Army has for the first time tested swarms of consumer drones during a major military training exercise and determined the low-cost technology is at a stage where it could be used offensively. By deploying swarm of consumer drones they become more viable as a weapon. They could easily overwhelm a small defensive position because they would represent too many targets moving too fast to successfully repel.

During the exercise, which is used by the Army to help evaluate new technology, the drones were deployed as a swarm to simulate a threat. In one exercise, for example, a swarm of drones with cameras on board was deployed in support of opposing forces in an attempt to discover the defensive positions of friendly soldiers.

Later, the Army expanded the trials to discover whether it might be able to make use of the same technology. The Army

tested flooding a chunk of airspace with a drone swarm to generate a disruptive radar signature.

“It has been proved that consumer [drones] can be used for intelligence, surveillance and reconnaissance, distraction tactics and, in the future, the ability to drop small munitions,” said Barry Hatchett with the Army’s Program Executive Office

## **Counter-Drone technologies**

Their low operational altitude along with small size, small RCS and small IR signature of the UAV makes it a difficult target for most of the common air defense systems such as anti-aircraft guns and shoulder-fired IR missiles.

Many drone detection and neutralization technologies are being developed from shoulder-mounted launcher system to physically capture it, silent cyber weapon that floors a drone instantly, anti drone cannons, Electronic Counter Measures (ECM) like jamming of command and control links and GPS spoofing, counter drone Directed Energy Weapons both laser based and electromagnetic weapons.

Most counter-UAS systems under development are focused on today’s threat, which relies on radio frequency (RF)-based remote control or global position system (GPS)-based navigation. However, the next evolution of sUAS will not require GPS nor active communications to accomplish their missions. These vehicles will be capable of navigating by visual means or other methods, performing synchronized actions that allow large groups to coordinate an attack against one or more moving targets and be used as intelligence assets or as weapons carrying platforms. An effective counter-UAS system must be able to defend against today’s and tomorrow’s threats in a range of operating environments and adapt to evolving sUAS technologies and tactics.

## **DARPA's Mobile Force Protection (MFP) program**

The Mobile Force Protection (MFP) program is an advanced technology prototype development program that will develop and demonstrate an integrated prototype system capable of defeating a raid of self-guided, small Unmanned Aircraft Systems attacking a high value asset on the move. This program will consider sUAS to be fixed or rotary wing air vehicles of less than approximately 200 pounds.

A sensing technology must be able to detect "numerous" small UAS at a distance of 1 km (0.62 mile) or greater and fit on a tactical ground vehicle such as a Humvee as well as the U.S. Coast Guard's Defender-class 25-foot boat, Darpa said. A neutralization system must disable or destroy numerous, self-guided UAS at a distance of 1 km or greater. Darpa describes self-guided UAS as rotary- or fixed-wing drones that do not rely on radio frequency control or GPS navigation for their operation.

To meet these challenges, the MFP program must develop and integrate affordable technologies into a prototype system that has the capability to complete an engagement sequence within a compressed timeline while mitigating collateral damage..

System affordability and adaptability to host platforms (ground and maritime) will be major system design drivers and allow for the deployment of an effective deterrent and defensive capability to protect the full range of potential DoD, Homeland, and private sector assets.

Given the rapid proliferation of the potential threat, DARPA seeks to develop a complete defensive system with a focus on mobility, affordability, and automation that can be fielded as soon as possible.

DARPA proposes a top-level system architecture that decomposes the CUAS engagement sequence into three steps – Sense, Decide, and Act – and envisions a “Neutralization Web” that flexibly ties the subsystems and algorithms implementing these steps into complete protection chains adapted to the operational environment.

An MFP system could include distributed and elevated sensors and effectors networked to form a fused air surveillance picture, be controlled for fast decisive action, and provide several low-risk UAV-neutralization options.

To demonstrate the system, DARPA experts will use the U.S. Army Maneuver Aviation and Fires Integration Application (MAFIA) as the backbone operating system to enable a system plug-and-play environment, and DARPA will consider only system prototypes that incorporate a MAFIA architecture. It is a Government-owned, Service-oriented architecture that supports multiple operating systems and provides services, libraries, common applications and a software development kit for performer integration

The MFP program will consist of three phases, each culminating in an open-air demonstration against continuously more sophisticated threats and challenging scenarios.

“DARPA is interested in identifying novel, flexible, and mobile layered defense systems and component technologies to address this increasingly important issue as well as conventional threats,” said Jean-Charles Ledé, DARPA program manager. “We’re looking for scalable, modular, and affordable approaches that could be fielded within the next three to four years and could rapidly evolve with threat and tactical advancements.”

## **DARPA selects three teams for Phase 1 of Mobile Force Protection programme**

Led by Dynetics, Saab Defense and Security USA and SRC, the teams were awarded Phase I agreements for MFP to develop a technology that is capable of detecting, identifying, tracking and neutralising adversary sUASs including fixed or rotary-wing aircraft.

DARPA Tactical Technology Office (TTO) programme manager Jean-Charles Ledé said: “Each team will now work to integrate novel ideas for advanced sensors and neutralisation approaches into a common framework emphasising safety for civilian bystanders, ease of operation, and low size, weight, power, and cost.

Our goal is a technology demonstration system that could fit onto currently deployed tactical ground vehicles and maritime vessels – getting advanced and upgradeable capabilities quickly to the warfighters who need them.”

The US Army’s maneuver aviation and fires integration application (MAFIA) service-oriented architecture has been chosen as the common framework for the data-fusion engine, decision-aid algorithms, and user interface for the teams’ command and control (C2) software.

MAFIA, which is already being used in several Defense Department (DoD) programmes, is said to support multiple operating systems and provide services, libraries, common applications, and a software development kit for performer integration. The MFP’s plug-and-play, technology demonstration system is anticipated to have the ability to integrate new sensors and emerging technologies.

“The three teams we’ve assembled have innovative ideas for a versatile, layered defense system that could protect convoys on the move from multiple small unmanned aircraft systems in real time,” said Jean-Charles Ledé, a program manager in

Darpa's Tactical Technology Office. "Each team will now work to integrate novel ideas for advanced sensors and neutralization approaches into a common framework emphasizing safety for civilian bystanders, ease of operation and low size, weight, power and cost."

## References and Resources also include:

- <http://www.militaryaerospace.com/articles/2016/11/drone-defense-moving-convoys.html>
- <https://www.fbo.gov/spg/ODA/DARPA/CMO/DARPA-PS-17-01/listing.html>
- <http://www.popularmechanics.com/flight/drones/news/a17371/record-breaking-drone-swarm/>
- <http://www.defenseone.com/technology/2017/02/counter-terror-chief-expect-terrorist-drone-swarms-soon/135736/>
- <http://www.defensenews.com/articles/dod-weapons-designer-swarming-teams-of-drones-will-dominate-future-wars>
- <https://www.sciencealert.com/swarm-home-made-drones-strike-military-base-first-attack-kind-russia-uavs>
- <https://www.ainonline.com/aviation-news/defense/2017-10-03/darpa-seeks-counter-drone-sensing-neutralization-systems>