Outline of a Counter UAV Philosophy

Lieutenant General P R Shankar, PVSM, AVSM, VSM (Retd)[@]

Abstract

The employment of Unmanned Aerial Vehicles (UAVs) in war and peace is proliferating rapidly. These are being used for offensive and defensive roles, to include surveillance, attack and logistics, besides other complimentary tasks. They are changing equations of conflict as was evident in the attack by a swarm of UAVs on the Aramco oilfields and ferrying of arms across the well fenced Indo-Pak border. Their role in non-contact warfare is increasing. In such a scenario, it becomes imperative that effective counter UAV systems are developed. As of now there is absence of a cogent counter UAV philosophy. Some counter UAV measures are being propagated and marketed in an inorganic and isolated manner. There is a requirement to have an overarching and holistic philosophy to counter the UAV threat. The counter UAV philosophy needs to be based on established threat patterns of adversaries. Thereafter, the vulnerabilities of UAVs have to be exploited to detect and locate them. Finally, one of the many kinetic/non-kinetic methods of their destruction have to be put into action. This article outlines such a philosophy from first principles in the near absence of any literature or reference material of significance on the topic.

Proliferation of Employment of UAVs

Usage and utility of UAVs is expanding in all walks of life to accomplish all kinds of tasks. In the military domain, UAVs were first employed for surveillance to look over the hill. Slowly but steadily, the roles of the UAVs have proliferated in the battlefield. They started out as surveillance platforms and have graduated to being electronic platforms for a large variety of uses. From defensive

platforms they have become very effective offensive platforms. The attack on the Aramco oilfields by a swarm of UAVs signifies a new strategic dimension in their offensive use. Earlier, UAVs were offensively used by USA to carry out precision and surgical attacks in Afghanistan and Iraq. They used sophisticated long-range UAVs like the weaponised Predator/Reaper for offensive tasks. These took off from air bases/aircraft carriers in the Gulf and were controlled by satellites from mainland USA. The prime example of such an offensive operation was the deadly surgical attack which eliminated Major General Soleimani in Baghdad airport. As against this, in the Aramco oilfield attacks, low cost explosive laden UAVs were used with an equally deadly effect. The differentiating factor is that the Aramco attacks caught a costly and sophisticated air defence system flat footed and looking foolish by completely evading it. While there have been instances of quadcopters having been used offensively in the Middle East conflicts, the dropping of arms using UAVs, through the smuggler network across the well-fenced Indo – Pak border, in Punjab, signifies a new facet of ingenious use of UAVs. It heralds the era of employment of UAVs for logistics. Logistic employment will expand as the capability envelope of the UAVs enlarge with shape and size. UAVs are now truly changing the dimensions of warfare.

The Form Factor of UAVs

Military UAVs come in various shapes and sizes. Largely they come in fixed wing or in quadrotor configurations. They also appear in the form of helium filled balloons; tethered or untethered. They operate from low altitudes right up to near space altitudes. Countries have already started exploring deployment options in near space. The major advantage of the UAV is that it is cheap, carries less escalation risk, is deniable, more flexible in employment, deployment and operations when compared to conventional manned aircraft. The employment options available in the military domain are manifold. They are unfolding at great pace, especially in asymmetric situations. We are just beginning to understand their utility in non-contact operations where deniability must be built in. As days go by, UAVs will dominate discussion on the battlefield. Equally, there will be a lot of discussion as to how to counter them. Armed forces have realised that they must defend themselves against this innovative and

ubiquitous third dimension threat. However, any form of defences against them need a very systematic and organised approach.

The Counter UAV Philosophy Approach

It is intended to present a broad philosophy and outline the entire range of counter UAV options to pick and choose from. This is an approach from first principles since there is very little literature available to refer to. Ideally, all the options should be adopted in a holistic, balanced and systematic manner if a comprehensive anti UAV system is to evolve for deployment in a military environment. Counter UAV operations in smuggling or other related security scenarios are not being discussed in this article. At the outset, a counter UAV system has three broad parts. Firstly, there must be an assessment of the UAV threat in each environment. Secondly, the task is to carry out surveillance and monitoring of the anticipated UAV threat as it unfolds. The third part is to deter, degrade or destroy the threat from enemy UAVs. An adjunct to this is regulating the usage of UAVs. This also must be given adequate thought.

Assessment and Appreciation of the UAV Threat

UAV threats from formal adversaries as well as from terrorists/insurgents/ non state actors must be assessed militarily. The appreciation starts with the UAV holding and capability of the adversaries. In our context, the holdings, characteristics and capabilities of UAVs held by China and Pakistan are of prime importance. We would also need to get a handle of how terrorists and insurgents can use UAVs and what their targets would be. It is mentioned that terrorists and insurgents favour Quadcopters and use them as surprise weapons to create out of proportion effects. It must be expected that Pakistan and China will employ UAVs aggressively since they have robust UAV programmes. Their UAV employment philosophy must be kept track of as it evolves. This must be followed by an assessment of the ground and weather conditions along our borders. It will give us a fair idea as to which UAVs can be used - where, when and how. For example, in conditions of rain, snow or high wind speeds in mountainous terrain, UAV operations are precluded. Similarly, in hot / turbulent conditions of summertime deserts and even high altitudes, UAV operations are difficult and limited. In cloudy conditions, satellite control of UAVs is not feasible. Hence depth of UAV operations is limited. UAVs cannot be flown in jet streams and that is a major seasonal and geographical constraint

in the Himalayas. It must be realised that most UAVs are relatively lightweight and low powered. Hence, their employment in adverse weather conditions, high altitudes/ mountains is quite predictable and will be confined to fair weather windows. Also, the range of operations of UAVs are restricted by communication ranges. These are in turn restricted by line of sight ranges. Further, as our adversaries continue to operate UAVs in peacetime, they are establishing a pattern in each area. The pattern will indicate timing, routes, heights, endurance parameters, exposure and so on. It is one thing to fly an UAV and another thing to carry out operational flying with a UAV. Hence, such demonstrated operational patterns define the broad envelope of feasible operations in each area. All UAVs must operate from some base. Hence, the infrastructure on the other side will give an indication as to how the threat can manifest itself. Presence of airfields, forward ALGs, widened roads, broad highways, corelated with characteristics of UAV, will indicate as to how the adversary will employ UAVs. It is also important to start monitoring the literary discussion which goes on in UAV related articles which appear in media. An assessment must also be made regarding the sources of procurement, technology and types of payloads, communication and other technical parameters. Finally, an assessment must be made of the intended targets of offensive UAVs. These targets would be soft and vulnerable. If these are attacked, the results could be spectacular and strategic. If all these issues are correlated sensibly as part of an intelligence plan, a clear threat picture will emerge. We will know as to what we are up against. It will also reveal chinks in the adversary's armour. Otherwise it will be a search in a haystack for the proverbial needle.

Monitoring, Detection, Identification and Surveillance

Vulnerabilities. Monitoring, detection, identification and surveillance of hostile UAVs is a prerequisite to countering them effectively. One should know where and when to deal with a threat before knowing how to deal with it. The problem is simple to define but widespread to crack. The UAV is a speck which can appear in a huge area despite the best of assessment. Hence, zeroing on to this speck at the earliest is the key. This can be done only through organised surveillance and monitoring. The principles of monitoring and surveillance are akin to other Air Defence (AD) surveillance system. In most cases, the larger and high-altitude capable UAVs will be caught by the Air Defence surveillance network. It is, however, the

low-level flying UAV which is difficult to detect. Detection of UAV(s) is feasible if we understand those characteristics which make them liable to be detected. Firstly, the UAV or a swarm of UAVs are a dead giveaway due to their sound. The constant high decibel whirring of UAVs cannot be hidden. Secondly, UAVs are slow fliers. Their movement is easily trackable unlike high speed manned aircraft. Thirdly, UAVs must be persistent over an area. Whether it is for surveillance of an area or for acquiring a target prior to attacking it, they must persist and spend time on target. In doing so they become detectable. Every drone has a form factor which in turn constitutes its radar cross section. Hence, radar tracking is a feasibility. Lastly, every UAV is a mass which is constantly receiving or sending electronic signals. These electronic signatures can be detected. Each type of surveillance needs a bit of further understanding.

Acoustic Detection. The acoustic signature of an UAV is unmistakable and cannot be hidden. The UAV can be tracked using a passive gridded network of acoustic sensors. Using the differential of sound intensity and time differentials of incidence of a sound wave at each acoustic sensor the UAV can be tracked with reasonable accuracy. Suitable algorithms for this correlation can be developed through simulation models. The good old principles of sound ranging used to locate guns is a logical start point. The best part is that the UAVs acoustic signature will not be swamped by other battlefield noises due to its distinctiveness. If a swarm is approaching, the detection will be even easier due to either cancellation or cadence of frequencies.

Electronic Signatures. Every UAV has a number of communication links to control its flight and payloads as also for data transmission. These will be ubiquitous all-round transmissions/ reception. Further, if it has an active payload like Synthetic Aperture Radar (SAR) on board, the radar will also emit. All these electronic emissions can be detected through simple electronic Direction Finder (DF) procedures. Through ingenious Electronic Warfare (EW) methods, it can also be detected as to what is the business of the hostile UAV and can be hacked into. It is in this context that the knowledge of characteristics of the UAV is important. The UAV has multiple electronic signatures which make it vulnerable.

Radar Detection. All UAVs, small or big have a radar cross section. Of course, with a small radar cross section and using under

the radar horizon low level flying tactics, the UAV tends to avoid detection. However, it does not mean that it cannot be detected. Continuous Wave (CW) doppler radars with phased arrays can detect high speed gun and mortar shells at more than 50 km away. Such radars can detect UAVs of most variety. Hence the existing Weapon Locating Radar grid must be dual tasked for location of hostile UAVs also.

Optical and Thermal Tracking. The time tested, simple and effective optical tracking method should not be discounted. One can use instruments like Long-Range Reconnaissance and Observation System (LORROS) and other optical systems to see and track hostile UAVs. These optical trackers could be part of a mobile/static observer network like any other AD system. The thermal signature of an Internal Combustion (IC) engine powered UAV can be detected by any thermal imager due to the high thermal contrast of the UAV engine against the background of the sky.

Passive and Active Tracking. In a very broad sense, locating any hostile UAV can be done either passively or actively. However, it has to be timed and cover a wide area as per threat assessment. Passive location systems will have to be the primary means of detection. An active system must zero on to the hostile UAV based on the pointers provided by the passive system. It should further be able to act in concert with offensive systems to destroy / degrade hostile UAVs. The passive and active systems must be deployed in a grid with adequate communications to be responsive to situations. UAV detection, surveillance and monitoring grids must be meshed with the existing AD surveillance system.

Destruction and Degradation of UAVs

General. Once a UAV is located and monitored, it can be destroyed or degraded, kinetically or non-kinetically. It can be tackled electronically or physically. Electronic methods are easier and effective options, specially against low flying electric powered UAVs which do not emit any thermal signatures. Against high level flying IC engine-based UAVs, physical and electronic options can be employed as per availability with equal effect. Both these options are discussed.

Electronic Degradation. Electronically every UAV can be interfered with. All UAVs have communication links to receive control

signals, send back data and receive GPS signals. These linkages can be jammed to degrade the UAV. Most UAVs have a safety feature which makes them return to base when their flying control signals are interfered with / broken. Once the control links are interfered, the UAV will return to base. Jamming the GPS receivers will render the UAV to go back to base or go awry. Interfering with the data channels will blind the UAV. A more sophisticated variance of this is 'spoofing'. Higher powered transmissions of frequencies than those used to control the UAV, or its payloads can be used to spoof and take over the UAV or even crash it to destroy it. There are methods available to do so.

Kinetic Destruction. Any UAV can be destroyed kinetically. The slow speeds of UAVs and their need to be persistent exposes them. Hence, they become vulnerable to kinetic / physical destruction by anti-aircraft guns, missiles or Directed Energy Weapons (DEWs). Larger UAVs and Balloons (tethered or untethered) are easy targets for existing AD systems once detected. Heat seeking missiles would be very effective against IC engine powered UAVs. The near space threat must be defeated physically with missiles. Lasers and high-powered microwaves can also be used against UAVs. Lasers can be employed to critically injure the UAV to make flying a difficult proposition. High powered microwaves will fry its electronics and render a UAV ineffective. There are also suggestions to use water cannons, nets and machine guns against low flying UAVs. However, these would be for really low flying objects. All in all, kinetic destruction of UAVs will be a 'horses for courses approach'.

Rules and Regulations

The UAV threat has assumed gigantic proportions since the sector is largely unorganised. Unless there are clear rules and regulations put in place and UAV operations come under a regulatory authority, very little knowledge will surface about the technologies and technical specifications of various UAVs. Clear rules, regulations and controls regarding UAV registration, usage, traffic, no fly zones, payloads allowed, communication protocols and so on will bring in transparency in the system. In turn, it will aid in detection and monitoring of UAVs in the hinterland, which will add to the effort of combating the hybrid and asymmetric threat. It will also go a long way in avoiding fratricide.

Anti Swarming

UAVs in a swarm are the new threat. Generally, UAVs in a swarm intercommunicate with each other. The swarm could be in an autonomous mode or in a controlled mode. In a controlled mode, the swarm would generally have one 'Queen Bee' controller. The swarm could be directed against one target or against multiple targets with each UAV in the swarm assigned to a task/target. A well-organised swarm is difficult to destroy physically, since destroying just one UAV or a few will not achieve the results required. It is best to electronically degrade the swarm by interfering with the intercommunicating system. If the controller or queen bee in the swarm can be detected, it should be targeted. However, it is easier said than done.

Effect on Own Operations

Many options are available to detect and neutralise UAVs and many more will come up in future. However, one of the most important issues is the effect such counter UAV operations will have on own air and electronic operations. The range of air operations include use of airspace by own aircraft, missiles, UAVs and Artillery. Care should be taken to ensure that counter UAV operations do not hinder own operations either during war or peace. Airspace management, frequency management, electronic silence and other restrictions will have a large role to play – not only in counter UAV operations but also in other routine operations. Hence command and control of counter UAV operations will have to be meshed in or be part of Air Defence operations in the larger scenario. Counter UAV operations can not be left in 'weapons free' mode lest they become fratricidal.

Conclusion

UAV operations are coming of age and the UAV threat is increasing by the hour. As the threat increases, the need to protect own forces and vulnerabilities against this potent game changing threat is also growing. However, counter UAV operations are at a nascent stage and are greenfield in nature. They are just surfacing and lack clarity in how to approach them. In any perspective, counter UAV operations must be a systemic approach and this must mesh in with existing Air Defence systems in the battlefield and with other civil systems which will evolve in future.

@**Lieutenant General PR Shankar,** PVSM, AVSM, VSM (Retired) is a former Director General of Artillery. He is an alumnus of National Defence Academy, Khadakvasala, Defence Services Staff College, Wellington, Army War College, Mhow, Naval Post Graduate School, Monterrey and National Defence College, New Delhi.

Journal of the United Service Institution of India, Vol. CL, No. 619, January-March 2020.