Tactical Pocket Reference
*A Guide for U.S. Forces*
March 2015

# Unmanned Aerial System (UAS) Threat Awareness

Asymmetric Warfare Group
2282 Morrison St. Ft. Meade, MD 20755-5355
SIPR: https://portal.awg.army.smil.mil
NIPR: https://newportal.army.mil
Email: usarmy.meade.tradoc.mbx.usarmy-ft.-meade-tradoc-list-awg-opcen@mail.mil




## Bottom Line

- The enemy's use of UAS means you have an air threat. Operate that way.
- The "Poor Man's" Air Force: UAS are cheaper to use than manned aircraft and can perform many of the same missions.
- Low, Slow, Small: These three attributes of UAS make them tough to detect on radar or even visually. Thus, UAS present a challenge for modern air defense artillery.

## Enemy UAS Mission

- UAS can be used to conduct Direct Attacks, Indirect Attacks, ISR, Cyber Warfare, to elicit reactions or any other combination limited only by creativity.
- Once spotted, UAS are vulnerable. Direct fire engagement is one option (be aware of collateral damage beyond the target).
- An option to consider is to use terrain analysis and the flight path of the UAS to determine the launch point and neutralize the controller.

## Find Enemy UAS

- Use Air Guards. Designate a person to observe above the horizon.
- Pay close attention at key times: Immediately after IDF attacks, during/after Key Leader Engagements, during/after raids.
- CoIST/S2 should determine if enemy UAS are establishing a pattern.
- All C2 elements should know who to call to determine if airspace is clear of friendly air.

## What Do I Do?

- Proper planning by leaders will ensure that units employ adequate force protection measures to counter the UAS threat. Units must develop TTPs to counter this threat in their respective areas of operation..
- Observe the threat (gather intel) or engage?
- Notify higher and adjacent units (Clear airspace and pass early warning).
- Move to overhead cover.
- Get distance and bearing to the threat.
- Take pictures. Use optics or handheld cameras.

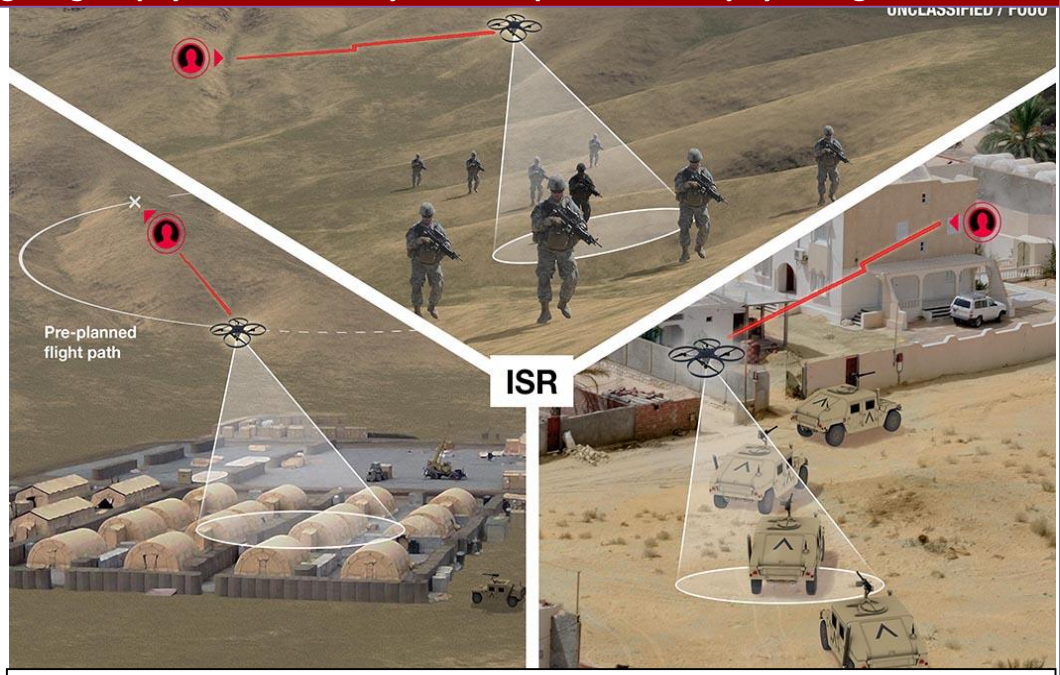
## Recommended Format for Reporting Enemy UAS

| LINE | INFORMATION EXAMPLE | Example |
|---|---|---|
| 1 | Unit call sign and frequency | Red 1, FHXXX |
| 2 | Unit location | 6- or 8-digit grid |
| 3 | Location of threat UAS asset | Grid or distance and direction from reporting unit location |
| 4 | Time threat UAS asset spotted/detected | DTG |
| 5 | Estimated time on site | Was threat UAS asset approach observed or was it spotted overhead? How long might it have been there? |
| 6 | Flight characteristics | Is threat UAS loitering in one spot (possibly already spotted reporting unit), is it flying straight (en route to loitering location), what is direction of flight, or is it flying randomly (searching)? |
| 7 | Estimated size, elevation, and physical description | Wingspan, height, color, tail configuration, |

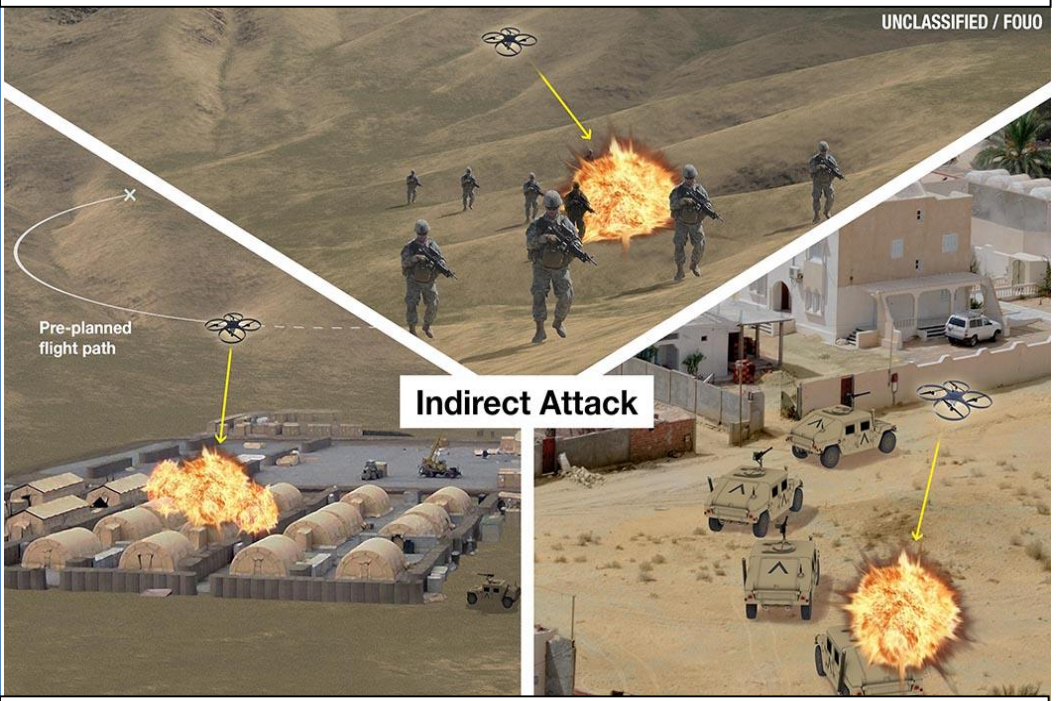
Reference: Infantry Magazine, May-June 2013

**Methods of employment can vary from active guidance to automatic or autonomous. Other methods can include trial / inert runs to elicit a friendly response for observation. Threat UAS can also facilitate Cyber attacks using a signal payload to covertly steal or spoof a friendly cyber signal.**

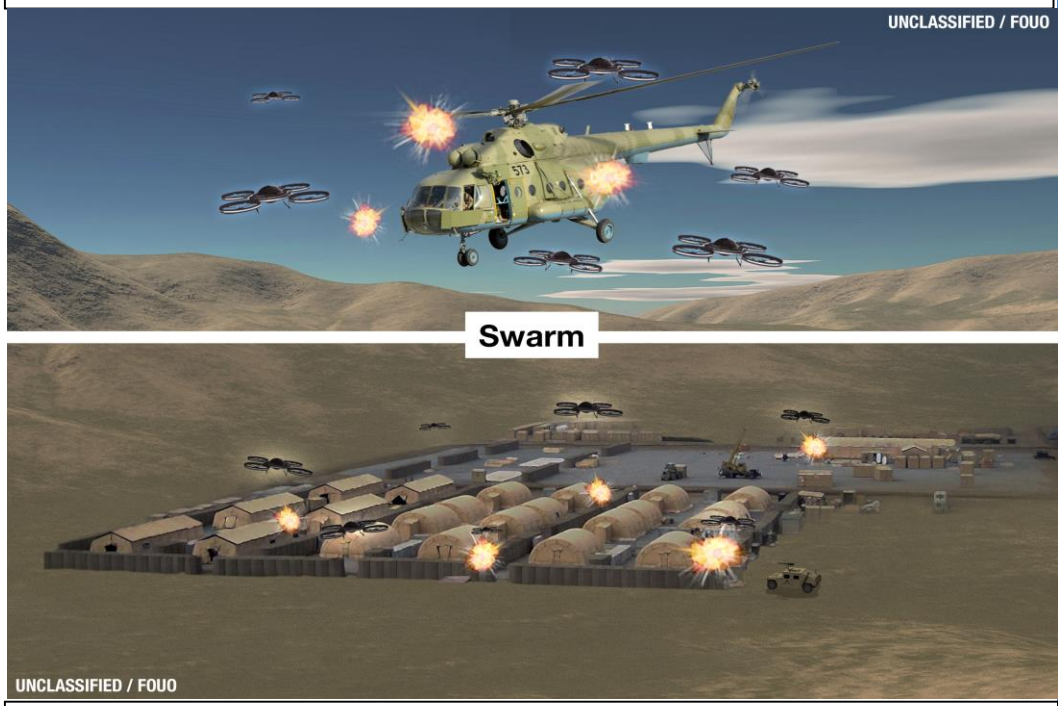

**Direct Attack:** UAS strikes target and causes damage or injury through force of impact or payload carried.




**Surveillance:** UAS gains situational awareness of friendly forces and activities or provides C2 and directs ground attacks through a video feed




**Indirect Attack:** UAS releases hazards (explosives, toxic materials, CBRNE, etc.) to cause damage, injury, chaos, or death.




**Swarm Attack:** Threat uses a swarm of UAS to cause significant damage and overwhelm friendly systems and reactions.