Counter-Drone Solutions: Do we know what we want and do we know what we are getting? A relatively light-hearted look at some serious questions.

You will not be surprised to read that nothing I am about to discuss is new or revelatory; the aim is purely to keep the debate going and perhaps remind those that need reminding, that there is always more to something than meets the eye.

The beginning.

With continued growth in the commercial sector and a steady private or hobbyist market, drones, and therefore the need to detect them, continue to provide authorities with real challenges. And they are just the unmodified ones. Couple those with the readily introduced modified COTS and hybrid home builds that are more likely to be used for illicit activity, and the problem of detection is somewhat exacerbated.

All of this leads to the most important component in the ensuing discourse, the customer. They must start from a point of wanting something.

I suspect that 'want', in the first place, is no more complicated than "I need something to let me know if my area of responsibility is being infiltrated by a drone (or drones) as they may be being used for nefarious activity".

Options.

OK, so you have a requirement. But what do you really want? Do you want a 'cheap and cheerful[1]' capability as reassurance to a higher authority that you are looking at the problem and you have a quick win solution? If that is the case, does the risk appetite accommodate the fact that your 'quick win' is highly unlikely to be a complete solution. How many holes in the cover are you happy to live with? How many can you afford to live with?

Are you happy to be overt with your approach to detection solutions? If you are, then your options increase. Multi-layered solutions that cover all options (radar, EO/IR camera, passive RF) may be considered the gold-plated solution, but then that comes at a price. Conversely, if you want to retain some semblance of covert operation (either full or partial), then that takes you down a different path.

And of course, is it sufficient for you just to know? (detect), or do you want to do something about it? (defeat); it's not long before what you want (or can afford) is directly proportional to the depth of your pockets.

[1] 'Cheap and cheerful' is not meant necessarily as a derogatory reference to quality and standards, but more in terms of an incomplete offering (although we all know that 'cheap and cheerful' does exist in the former sense).

Consequently, and fundamental to all of this, is the requirement to understand the potential false economies when evaluating short term quick wins with long term effectiveness.

Smoke and mirrors?

Everyone in the C-UAS field is rightly protective of their technologies. We have all taken a 'sharp intake of breath' over the latest and greatest claim. Is it because we do not know? (and are frustrated that someone else got there first), or is it because we do not believe, as what we are reading flies in the face of the science that we do know? How we choose to justify our approach to that position will likely bias us towards one route or another and the questions we should be asking.

Long arm of the law.

With the planned introduction of Remote ID[2] legislation by both the CAA and FAA, it is almost certain that there will be numerous means by which we can detect, track and identify the majority of drones being operated by law abiding drone users relatively easily. It will be the law in the UK and US, and I propose that as a large proportion of the drones produced in the world will be for those markets, then it is highly likely that most of the drones produced worldwide will be built with inherent Remote ID.

However, is it the law-abiding drones we are predominantly bothered about? I suggest not. Consequently, all the systems that will be being produced to interrogate the Remote ID, and which are likely to be lower priced, mass produced sensors, will not provide an effective capability against the ardent hostile agent, criminal mastermind or terrorist operative. At best it can be said they may help. At worst, they will provide the customer with a false sense of security, whilst providing the 'bad guy' with a hole to fly through.

What about using a capability that interrogates the drone control signals and decodes the data, thus providing drone ID information from the embedded data? That type of hacking capability is strictly controlled (and if not done correctly is illegal); at the very least it is subject to compliance with stringent legal statutes within the country of use. That very fact is likely to be high in the mind of those manufacturers that currently provide manufacturer specific drone detection solutions……. Or is it?

Questions, questions.

You have opted for a sensor that has a library. That must be good? What does that library cover? 80%, 90%, 95% of known drones? What about the others?

"It's no problem" I hear in response to that latter query, "we can add new targets when we get them" (after having identified the RF signal (or mapped the RCS of the drone), deconstructed it, rebuilt it, tested it, loaded it into the library), "and we use Artificial Intelligence (AI) to assist!". OK, sounds plausible; but it is still a library with holes in it.

[2] Remote ID will include location, altitude, direction, and speed information as well as operator ID details.

It is also worth acknowledging that drone manufacturers are very protective of their control signals and potential vulnerabilities. Moreover, because of that and the fact that manufacturers are so concerned that in certain instances they are formally paying 'hackers' to identify bugs (that can then be resolved), we must accept that there will be a constant and rapid evolution of control signals. Therefore, the associated question that needs asking is how long does it take to 'break' a new control signal? Assuming the drone manufacturers are not going to freely handover their technology, current passive RF sensor technology will continue to rely on getting hold of the new drone signal technology, exploiting it, and placing it in a 'library' of sorts. Consequently, exploitation of new control signals (legal or otherwise) for use in a passive RF drone detection capability will remain time consuming and therefore such sensors that rely on a database library will always be behind the drag curve.

It's probably also appropriate at this point, seeing that I've introduced AI at the beginning of this sub-section, to ask the question of whether AI really is the panacea?[3]

It is certainly a well-used, if not over-used, buzzword (or abbreviation) that gets banded around along with Machine Learning (ML). But does it deliver (at the moment) as quickly and as effectively as those that use the term(s) believe it should? How long does it take, using AI, to create new database/library entries? Are we talking AI assisted detection algorithms or AI assisted automatic alert (and control of effectors – oops, didn't want to jam that!)? Currently, there certainly remains a case for some form of 'human in the loop' intervention. For how long though, remains to be seen.

Food for thought.

I hope my musings have given you something to reflect upon. As I said at the outset, it is nothing new, but definitely well worth a few moments of contemplation. If nothing else, it will hopefully provoke you into asking more questions.

Andy Smith
Business Development Manager
METIS Aerospace Ltd

About METIS Aerospace Ltd www.metisaerospace.com

METIS proudly manufactures and delivers the SKYPERION range of modular and scalable passive RF Drone Detection sensors and control software, providing a proven, cost-effective, Detect, Track and Identify solution. Available in several formats (fixed, mobile, portable), SKYPERION can also be easily integrated with effector capabilities and C2 entities as part of a fully layered C-UAS system.

[3] I'm asking the question, not answering it!