ProtectUK

Countering threats from Uncrewed Aerial Systems (C-UAS)

Original publication date
02/11/2020

1. Introduction

There has been a significant growth in the legitimate use of Uncrewed Aerial Systems (UAS) over recent years. This is anticipated to increase as the potential uses of UAS continue to develop. It has been estimated that there could be over 76,000 commercial drones in UK skies by 2030 and are expected to deliver considerable economic benefits to the country. However, as their use increases and develops, security risks are also emerging.

Overseas, terrorists are using UAS in conflict zones for surveillance, propaganda and to deliver improvised explosive devices. In the UK, UAS pose an evolving threat. The 2018 Gatwick Airport drone incident highlighted the disruption that can be caused by a hostile UAS incident. Disruption also continues to be caused by operators or pilots who are simply unaware of the regulations around

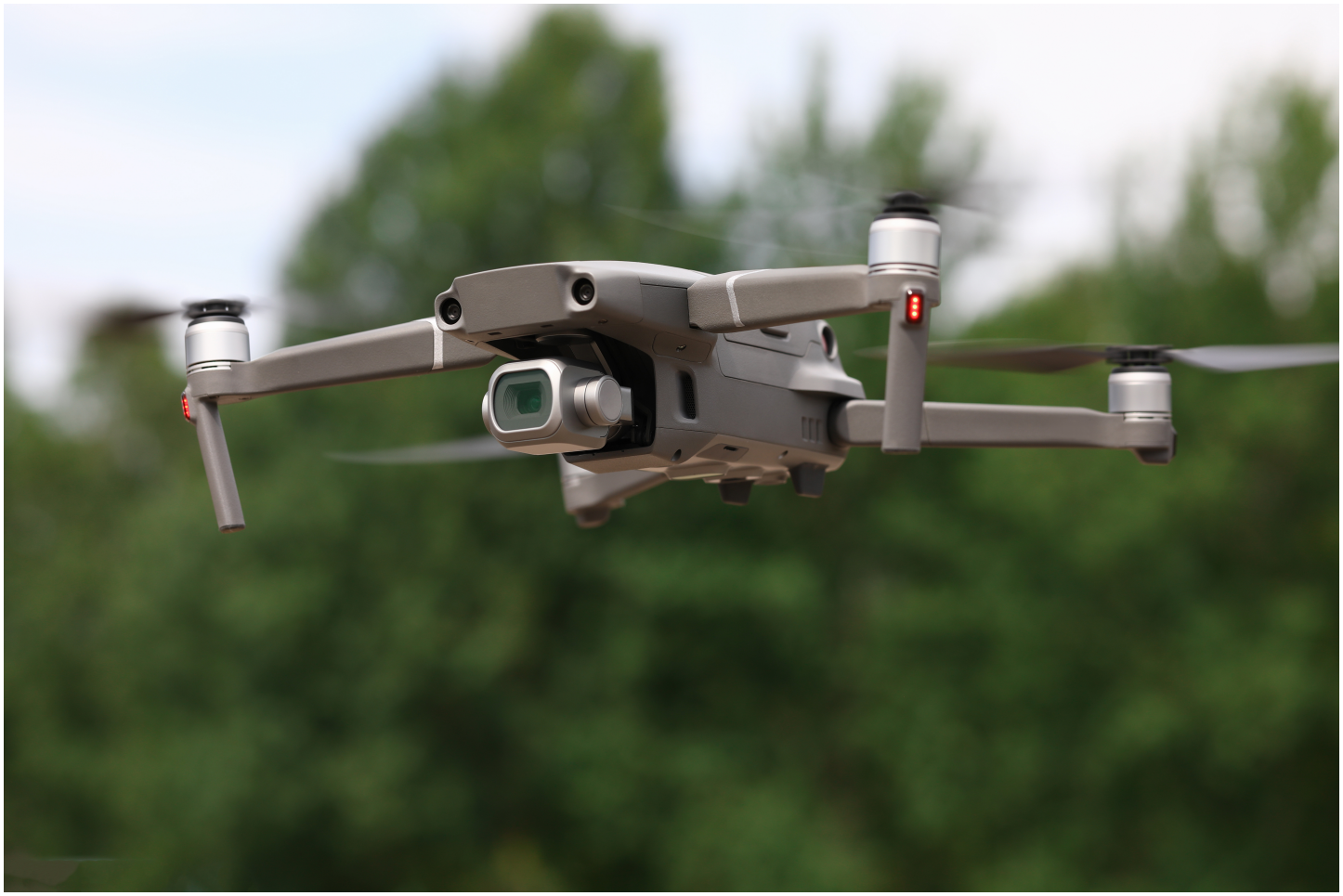
flying and fly their UAS in a negligent or reckless manner that may unintentionally cause danger or disruption. More broadly, the number of suspicious incidents in the UK is increasing, with over-flights of critical and sensitive sites now common place, and their use in carrying out unlawful protest increasing.

Sites need to consider the potential security risks posed by UAS and introduce appropriate mitigations. This guidance is intended to assist those responsible for the security of sites in understanding the risks posed by UAS and enable them, where necessary, to start to consider how they can introduce adequate and effective measures that mitigate the risks. The approach requires the development of a Counter-UAS plan, the components of which are outlined in the following sections. Each section will provide an introduction to the tasks that should be considered in the development of an effective plan. The development of this plan must acknowledge and integrate with wider protective security measures and overall operation of the site.

2. What is a UAS?

Uncrewed Aerial Systems (UAS) are systems that are comprised of three key components:

1. An Uncrewed Aerial Vehicle (UAV) that can operate without a pilot being on-board
2. A Ground Control System (GCS) which allows the pilot to remotely control and/or monitor the operation of the UAV
3. A bi-directional link between the UAV and the GCS which provides control, status and imagery information. A more competent user may fly pre-programmed flights via a phone, laptop or tablet. UAS describes the whole system. They may be of a fixed wing or rotary wing design, all of which are operated remotely



3. Building a C-UAS strategy and plan

As Counter-UAS mitigations are considered, it is necessary to make sure that they link into existing security plans. This may involve adding the UAS related risks into the overarching site security risk assessment and updating the associated security strategy.

This will ensure that the risks posed by UAS are considered in a manner proportionate to the other site risks and the solution is integrated into the overall security strategy and site operations.

A site Counter-UAS plan will need to be developed which will determine what needs to be done to reduce the risk of unauthorised UAS incidents.

3.1 Governance

Key decisions will need to be made at the highest level of an organisation as a plan is developed. It is important that senior decision makers understand the UAS risk that has been identified and the

options as to how they could be mitigated.

3.2 Stakeholder engagement

Early identification and engagement with internal and external stakeholders are important at each stage of the development of a Counter-UAS plan, from assessing the risk, through to developing appropriate responses. Agreement must be sought in relation to the roles and responsibilities of all those involved.

Engaging with the appropriate regulators should also be considered. Local organisations whose sites are nearby, or have shared use of the site being protected, are also likely to play an important part in developing and delivering the plan.

3.3 Engagement with the police

As with all matters relating to security and policing, a strong relationship with the police built on understanding and compromise is key. Your contact may be with either the local police or those specifically tasked with providing policing to certain sites. It is important to identify the contacts who may be able to support the development of the plan. This could include providing support: in developing an understanding of the risk to the site, provision of guidance in relation to the mitigation of the identified risk and the development of the overall plan. This engagement will be vital to building a plan that delivers an effective, co-ordinated and proportionate response to any suspected unauthorised UAS activity. In determining the level of response to any incident, the police will need to assess the threat, harm and risk against the resources they have available.

The relationship should seek to cover the following:

- how the police may support the development of the plan
- the technology the site has in place and how this is used
- the development of reporting and response processes
- the actions the site should take in relation to seizing drones
- testing and exercising
- training and guidance for staff
- developing a policy on supporting prosecutions and ensuring processes are robust enough to achieve a successful prosecution

Early engagement with the police is recommended in relation to one-off events, where the security risk is raised for a short period of time. This may be as a consequence of the attendance of protected persons or the nature of the event taking place.

3.4 Analysis of previous incidents

Valuable learning can be gained from understanding how UAS have previously been used maliciously and the effectiveness of the response at different sites. These incidents will provide information that will both inform the threat and enable sites to learn from how incidents have been managed.

4. Assessing the threat and risk

The first step in developing a Counter-UAS plan is to review the site's strategic security risk assessment. This should include a high-level assessment of the security risks posed by UAS threats to the site and should involve an assessment of the threat, vulnerability and impact of a UAS incident. The risk assessment should be used to identify what mitigation the site needs to put in place.

The threats that can occur at each site vary considerably. Methods of hostile activity that UAS are used for at a site include:

- to cause disruption
- undertake surveillance
- delivery of a payload

A variety of threat actors have been seen to use these methods and may include:

- hostile state actors
- terrorists
- criminals involved in either serious and organised crime or lower-level crime
- protesters – conducting unlawful protest
- journalists and others conducting unauthorised surveillance
- negligent and reckless users

The site security and safety risk assessments should be used to identify the threat scenarios that are

likely to present the greatest risk to a site as they vary considerably. Decisions made in relation to Counter-UAS mitigations need to be proportionate to decisions made in relation to other security risks to the site.

Your local CTSA may be able to assist in assessing how the threat manifests in relation to your site. It should be noted that UAVs being flown across sites that do not have airspace restrictions and where the pilot is operating within the limits laid down in the Drone Code may be operating lawfully.

More information on the Drone Code can be found on the Civil Aviation Authority website.

4.1 C-UAS vulnerability assessment

A site vulnerability assessment for UAS threats should be completed, to inform the detailed risk assessment and the Counter-UAS plan. It will also provide information in relation to:

- the threat scenarios posed by UAS that are most relevant to a site
- the type of UAS which might be used and how they may be used
- the vulnerability of key assets
- where the likely launch points are situated

Analysis should also be undertaken in relation to any historic UAS activity in and around the site. This will provide useful information as to what can be expected in relation to both UAS leisure use, but also any historic hostile use.

5. Reducing negligent and reckless use and deterring hostile activity

The vulnerability assessment will inform a range of security measures which are intended to reduce the risk of negligent and reckless UAS use and deter hostile activity, including:

- local business and community engagement
- security minded communications
- airspace restrictions and/or geo-fencing

These measures provide a base layer of mitigations and allows sites to consider what further protective security measures are necessary to deal with hostile users and justify a more robust response to these incidents.

Consideration should be given as to how each of these concepts can be incorporated within the plan.

5.1 Local business and community engagement

Engagement with local businesses and the community can be used to raise awareness of the threats posed by UAS and assist the community in understanding what they can do to help mitigate these risks.

Time will need to be spent identifying each stakeholder group and deciding how they should be engaged.

5.2 Security minded communications

Corporate communications should be developed and used to help:

- deter potential malicious individuals from attempting to use UAS
- reassure the public and local community by promoting the efforts of the organisation and authorities to ensure their safety and security
- recruit the local community and the public to be part of the detection effort
- engage with all internal staff to increase their awareness of the threat from UAS

Showcasing, via the usual communications channels, that local communities are vigilant and reporting unusual activity can encourage further reporting. Critically, this can also help deter malicious individuals. It may be appropriate to erect signage prohibiting the use of UAS at points of access to identified likely launch sites and nearby transport links. Customised signage, leaflets and posters are available from your local police CTSA.

Communications should be developed to increase the awareness of all personnel working on a site to the potential risks UAS pose to them. This will develop their understanding of the threat and how it may occur locally, preparing them for the actions they should take if they witness an incident.

Communications should:

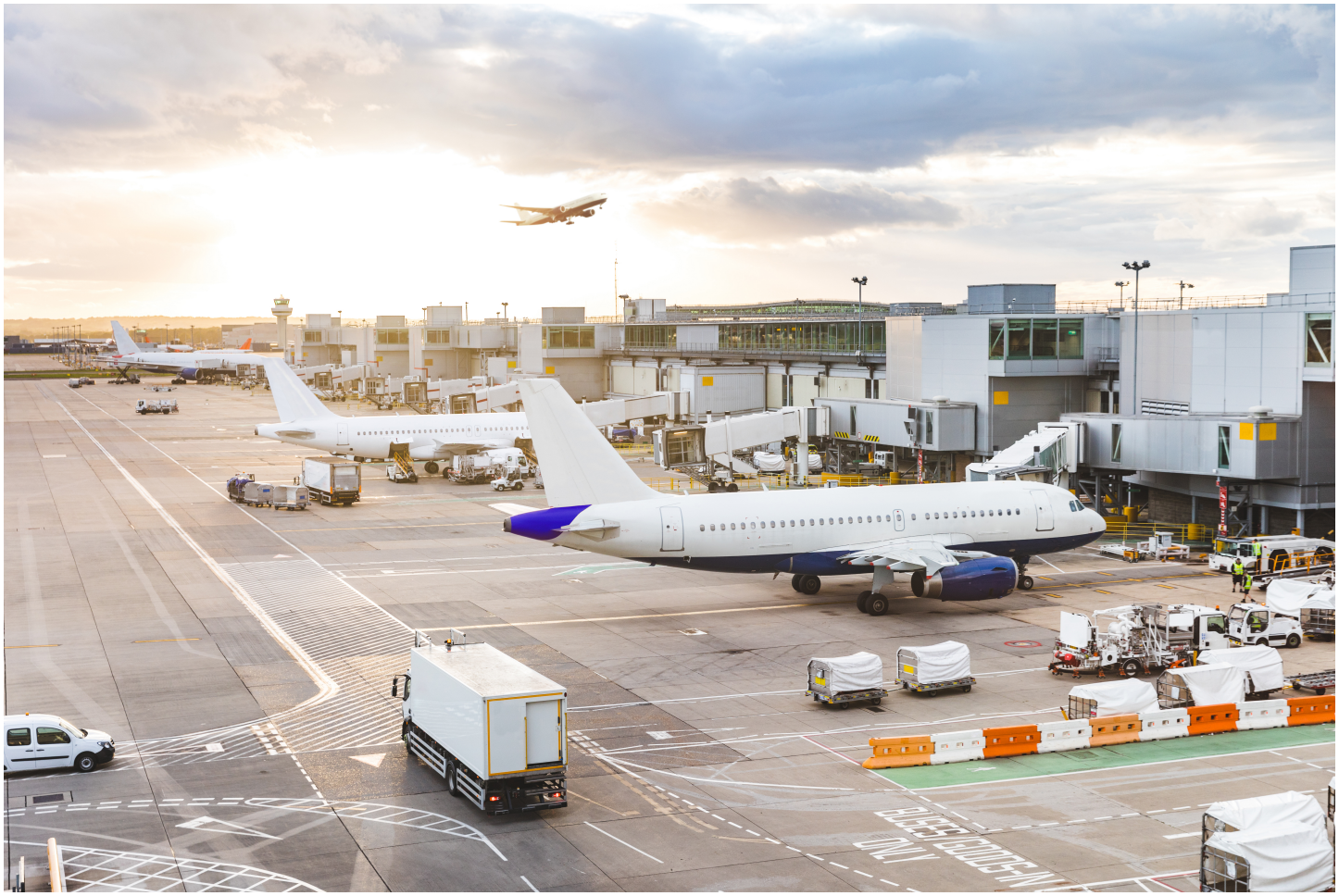
- ask personnel to report any unusual behaviour or activity – trust their instincts
- give clear instruction on how and what to report (e.g. phone number and description)
- crucially, deliver confidence that reports will be taken seriously and will be investigated

For further information, read more about Hostile Reconnaissance.

5.3 Airspace restrictions

The UK has a well-established system for notifying blocks of airspace where particular limitations are placed on the flight of all aircraft (manned and uncrewed). It is also possible to place a temporary restriction on airspace, either as a result of a pre-planned event, or in reaction to a short notice occurrence, such as an emergency incident.

Organisations should use the Civil Aviation Authority (CAA) website and associated apps to identify which type of airspace their site is located in. Further information on airspace restrictions can be found on the CAA website, and there are an increasing number of apps available for UAS operators to use to identify potential hazards while flying.



5.4 Geo-fencing

Geo-fencing is a virtual barrier around pre-defined areas of airspace. It is manufacturer specific and therefore has no effect against UAVs manufactured by others. Geo-fencing will not stop a determined malicious actor; however, it is useful for helping sites identify intent and reduce negligent and reckless use.

Further information on geo-fencing can be found on the NPSA website.

5.5 Authorised UAS use at your site

Many sites are increasingly using UAS for a wide variety of legitimate and useful activity. Consideration must be given to how a site manages authorised UAS activity. It is important that any planned UAS activity is reported in advance, so that it can be de-conflicted against any suspicious activity. There should be a single point for reporting and recording such activity.

6. Physical hardening

Physical security hardening should be considered at an early stage of Counter-UAS planning. The vulnerabilities identified in relation to the key assets during the vulnerability assessment will determine the need to consider where and how physical hardening can be used. Straightforward and less expensive measures to help reduce the risk of negligent and reckless use should be adopted at the first opportunity. Other more complex measures such as creating physical barriers may need to be considered when a higher level of risk has been identified.

Physical security measures can be introduced to help protect the asset through, for example, concealment, disguise, preventing physical access or hardening. The selection of the physical security measures will depend on the risks.

Consideration should be given to making launch sites in the immediate vicinity of key assets less appealing by introducing cover from view, adding lighting and controlling or restricting access.

7. C-UAS technology solutions

A Counter-UAS technical solution is intended to provide:

- early warning that an unauthorised UAS is approaching or within a site
- a rapid tasking of operational and technical resources to respond to an incursion
- information to enable decisions as to the safe operation of the site during and after any incursion
- evidence that will support the investigation and prosecution of offenders

A technical solution will enable more informed decisions to be made when responding to an incident.

Organisations wishing to use this technology should make sure they understand its performance, the legalities of its use, and the unintentional consequences and collateral damage which may be caused.

Sites should only be considering the use of technical counter measures once they have drafted their Counter-UAS plan; introduced measures to help reduce the risk of negligent and reckless use; and determined that the risks to the site have still not been adequately mitigated.

Counter-UAS technology requirements should reflect the security risks that each site faces. They must be proportionate to the risk and other safety and security measures that are present to protect the site. They will need to consider the continuing and rapid developments in both the UAS and the Counter-UAS technology market.

8. Types of C-UAS technology

Broadly speaking, Counter-UAS technology comprises two main types:

- Detect, Track, Identify (DTI) Technology that can be used to detect, track and/or identify a UAV and/or Ground Control Systems (GCS), the primary purpose of which is to provide security personnel with the timely and accurate information they require to enable a proportionate and effective response
- Detect, Track, Identify, Effect (DTIE) Technology that can be used to provide security personnel with the timely and accurate information they require to enable a proportionate and effective response which includes using a technical effect to prevent the UAV from completing its intended activity

9. Identifying the requirement and developing an operational requirement

(or) for C-UAS technology

Once it has been established that there is a requirement for a Counter-UAS technical solution, it is important to give detailed consideration as to exactly what is needed from the technology and how it will support the overall Counter-UAS plan.

Further information on the different types of technologies currently available, the capabilities and limitations of each, and considerations in relation to the deployment of such systems is available and should be sought prior to commencing detailed planning.

In order to ensure that the technology a site selects is effective, it needs to have undergone rigorous scientific testing. The testing should seek to understand the relative performance of a system within a controlled environment.

10. C-UAS operations

The activities already described in relation to local community engagement and security minded communications help build awareness of the threats posed by UAS and encourage the local community and site staff to report UAS related incidents.

For any threat to an asset, it is important to develop:

- a patrol plan for steady state operations that will act to both detect and deter unauthorised activity
- reporting processes that enable the collection of key information
- a dynamic threat assessment process to help determine an appropriate response on the basis of the information gathered
- response plans that are proportionate, effective and lawful, each having clear lines of accountability for decision making
- an exercise plan that will test the capabilities being developed
- a concept of operations that define how the response to any incident will be delivered, bringing together people, policies and technology

10.1 Steady state operations

The vulnerability survey should be used to identify areas around and close to the perimeter where a

UAV could be launched, as well as considering how security personnel and CCTV can be used to patrol these sites. These same locations may again become a focus of attention if there is an incident.

11. Encouraging reporting

11.1 Incident alerting

Detailed consideration must be given to encourage rapid and accurate reporting from both site personnel and members of the local community. Information should be provided to them on how to report an incident. This may include who to call and the information required.

As referred to previously, ‘No drone zone’ signage may be used to provide information on how to report an incident. The vulnerability assessment will assist in identifying the most likely launch locations and other places where signage is likely to be of most benefit.

11.2 Gathering accurate information

Staff should be briefed and trained in the information required should they suspect they have seen either a UAV or a GCS.

Pocket reporting cards may be used to provide a summary of the information a witness needs to collect and details of the number they should call. They should be provided to key staff who may either witness a UAV flight or be approached by a witness.

If a number of incidents take place over a prolonged period, then consideration should be given as to how the information in relation to each report is gathered and analysed. It will be important that reports are deconflicted, the information assessed and a picture built that will inform the response plan.

Depending on the nature of both the site and the incident, other stakeholders or agencies may need to be passed the key reporting information. This may help ensure it is appropriately assessed and improve the chances of the most appropriate response.

12. Operational response

12.1 Developing a response plan

A UAS response plan should cover, as a minimum, how to respond to:

- reports of UAS sightings or individuals suspected of flying UAS
- actions following the confirmed presence of a UAV or an operator
- the discovery of a UAV or related equipment

An initial plan should be developed as soon as possible. It should then be revised and developed as new mitigation is introduced or the threat changes.

The need to develop a clear understanding of individual roles and responsibilities is of considerable importance in relation to both the reporting and response to an incident. Internally it will be necessary to agree which department has responsibility for leading the response and how others support and enable this. Consideration should also be given to how the response is co-ordinated with the police. Guidance should be obtained from your local CTSA in relation to the actions that should be taken upon discovering either a pilot operating a UAS, or a UAV that has been recovered.

12.2 Responding to reported sightings

During a UAS incident, it is likely that there will be very little time to formulate a response and determine the intent of the operator. It is therefore critical to have well-rehearsed Standard Operating Procedures (SOPs) in place to make sure the most useful information is gathered and assessed at pace and made available to the decision maker. This will help them implement a predetermined and proportionate response.

The best available information should be gathered from available sources to enable effective decision making. This will include information from witnesses and, where available, the Counter-UAS technical solution.

In making decisions, consideration should be given to the following:

- the available intelligence and information
- assessment of the threat

- the available options
- what action to take

In line with the strategy, the response plan should set out the roles and responsibilities of the different stakeholders that will be involved in responding to a UAS incident. This includes, but is not limited to:

- taking decisions on how to respond
- considering the implications for current site operations including the safety of the people on site
- deployment of the security guard force and others
- engagement with police and other external stakeholders
- crisis communications, including appropriate messaging to staff and/or the public

12.3 Recovering suspect UAS

The response plan needs to incorporate what should happen if a UAS is recovered, or a report is received of a grounded UAV or UAV related equipment. Consideration should be given to:

- the health and safety related risks to staff and members of the public
- the opportunities that may be presented to recover forensic evidence of any offences

12.4 Testing and exercising

Testing and exercising (through table-top and live exercises) should be used to establish the viability of each element of the response plan and assure the enduring readiness of the people, processes and technology required to implement it.

It is particularly important the police are invited to participate in the testing and exercising of plans at an early stage.

13. Summary

The information set out above has introduced the issues that must be considered when developing a Counter-UAS strategy and plan.

Additional and more detailed guidance is available (see below). It must also be highlighted that the UAS environment is subject to considerable change in technology and legislation which impacts on their operations. The threat of hostile UAS activity is likely to develop.

For further information and detailed advice on countering the threat of UAS and the development of your plan:

Contact your local police CTSA.

Go to the CAA UAS webpage

Go to the NPSA C-UAS web pages

KEYWORDS
TERRORIST THREAT
ATTACK METHODOLOGY
PROTECTIVE SECURITY
RESPONSE
PALS GUIDANCE
PALS
PUBLICLY ACCESSIBLE PLACES
PUBLICLY ACCESSIBLE LOCATIONS