Countering Threats From Unmanned Aerial Systems

Making Your Site Ready

Published: August 2020

Classification: Official

CPNI
Centre for the Protection of National Infrastructure

EXECUTIVE SUMMARY

An introduction to developing a site specific Counter-Unmanned Aerial System (C-UAS) strategy and plan. This document provides information that will support the development of a protective security solution to combat the risks posed by Unmanned Aerial Systems (UAS).

- The risk to UK sites from hostile UAS use is growing. The starting point for building a UAS protective security solution is the development of a C-UAS security strategy and plan. Mitigations are available to reduce this risk.
- The C-UAS plan will enable the identification of UAS risks to the site, delivering appropriate and proportionate mitigations that integrate effectively with site operations.
- A framework is provided for the development of the C-UAS strategy and plan. This sits at the centre of a series of supplementary guidance documents that provide more detailed information about the individual elements of the plan.
- A range of counter measures are discussed that a site can introduce to mitigate the risk of UAS threats. These include: how to reduce negligent and reckless UAS use, physical hardening, an introduction to technical options and how to develop an effective operational response.

Disclaimer

The information contained in this document is accurate as at the date it was created. It is intended as general guidance only and you should not rely on it. This information should be adapted for use in the specific circumstances required and you should seek specialist independent professional advice where appropriate before taking any action based on it. To the fullest extent permitted by law, CPNI accept no liability whatsoever for any loss or damage incurred or arising as a result of any error or omission in the guidance or arising from any person acting, relying upon or otherwise using the guidance. Full terms and conditions governing the use of this guidance are available on our website at www.cpni.gov.uk.

INTRODUCTION

Intended readership

This document is intended to be read by those responsible for the protection of National Infrastructure (NI) sites, sensitive sites and crowded places. It is most useful for:

- Site Security Managers.
- Physical Security Managers.
- Security Control Room Managers.
- Business Continuity Managers.

Many of the concepts will have applicability to major events; however, there will be some differences. Much of the learning incorporated within the document, in relation to threat and risk, has been gained from analysis of hostile UAS activity that has taken place across the world. However, it is not intended that this guidance will counter the UAS threat that is manifested overseas. The use and mitigation of the threats posed by military UAS capabilities are also excluded.

There has been a significant growth in the legitimate use of Unmanned Aerial Systems over recent years. This is anticipated to continue as new and innovative uses are found and the capabilities of UAS continue to develop.

It has been estimated that there could be over 76,000 commercial drones in UK skies by 2030. These are expected to deliver considerable economic benefits, with net cost savings of up to £16 billion by that time[1].

However, as their use expands 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 now pose an evolving threat.

The incident at Gatwick Airport in December 2018 highlighted the disruption that can be caused by a hostile UAS incident. Disruption also continues to be caused by users who are simply unaware of the regulations and fly their UAS in a negligent or reckless manner that may unintentionally cause danger or disruption.

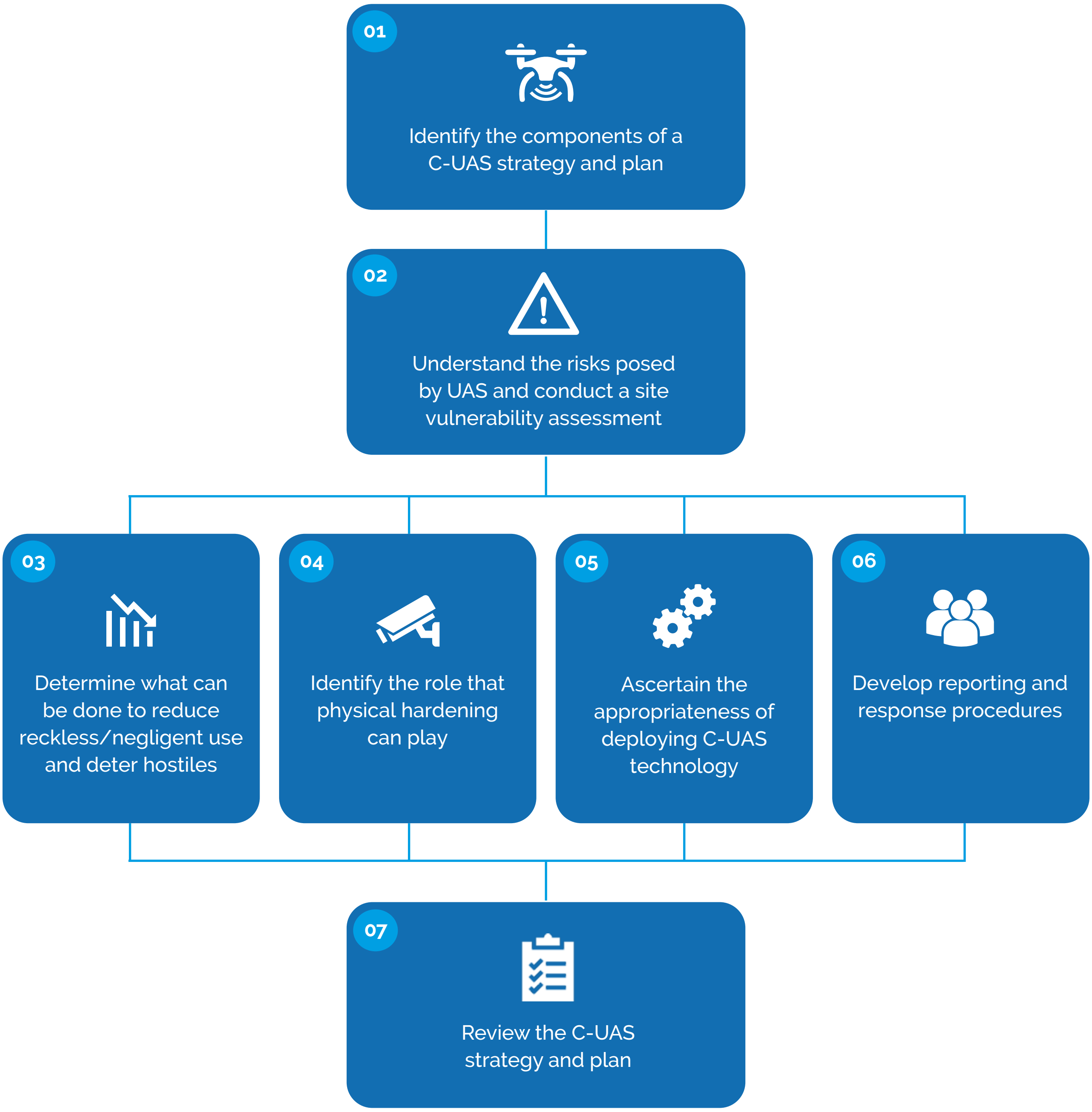
More broadly, the number of suspicious incidents in the UK and around the world are increasing, with over-flights of critical and sensitive sites now common place, and their use in conducting unlawful protest increasing.

[1] As quoted in House of Commons Science and Technology Committee report "Commercial and Recreational drone use in the UK", printed 8/10/2019

Scope

Sites need to consider the potential security risks posed by UAS and introduce appropriate mitigations. This document is therefore intended to assist those responsible for the security of sites in understanding the risks posed by UAS and enable them, where necessary, to introduce adequate and effective measures that mitigate the risks.

The approach requires the development of a C-UAS plan that covers an appropriate range of possible threat scenarios, the components of which are outlined in the following sections. The development of this plan must acknowledge and integrate with wider protective security measures and overall operation of the site. The document is divided into 7 sections, with the sections covering the tasks identified in the diagram below.



01 Identify the components of a C-UAS strategy and plan

02 Understand the risks posed by UAS and conduct a site vulnerability assessment

03 Determine what can be done to reduce reckless/negligent use and deter hostiles

04 Identify the role that physical hardening can play

05 Ascertain the appropriateness of deploying C-UAS technology

06 Develop reporting and response procedures

07 Review the C-UAS strategy and plan

What is a UAS?

Unmanned Aerial Systems (UAS) are systems that are comprised of three key components. These include the Unmanned Aerial Vehicle (UAV), the Ground Control System (GCS) and the bi-directional link between the UAV and the GCS.

There are many different types of systems available on the market which support both leisure and commercial uses. The technology is rapidly developing and continues to improve in terms of capability and affordability, inevitably creating additional security challenges.

01

An Unmanned Aerial Vehicle (UAV) that can operate without a pilot being on-board.

+

02

A Ground Control System (GCS) which allows the pilot to remotely control and or monitor the operation of the UAV.[2]

+

03

A bi-directional link between the UAV and the GCS which provides control, status and imagery information.

=

UAS

UAS describes the whole system. They may be of a fixed wing or rotary wing design, all of which are all operated remotely.

[2] A more competent user may fly pre-programmed flights via a phone, laptop or tablet.

01

BUILDING A C-UAS STRATEGY AND PLAN

Any site considering the risks posed by unauthorised UAS use is likely to have a framework of security products in place.

These will include: a security strategy, a security risk assessment and a range of mitigations and plans in place to reduce the risk of a broader range of threats.

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

This will ensure that the security risks posed by UAS are considered in a manner which is proportionate to the other security risks manifested to the site.

A site C-UAS plan will need to be developed and included within the framework. It will determine "what" needs to be done to reduce the risk of unauthorised UAS incidents.

All sites should look to identify the threats posed and implement appropriate mitigations. Not all mitigations will be required at every site – the choice will depend on the unique risks identified and the operating environment.

If there is shared use of a site, the security and C-UAS plan may need to be adopted by multiple organisations. There are a number of reasons for this:

- Resources are effectively and efficiently used and there is no unnecessary duplication of effort.
- All incident reporting is assessed in a single location so that the richest assessment can be made.
- There is a rapid and coordinated response with no conflicting activity. When an incident is underway there will simply be no time to confer between control rooms to agree a course of action. A predetermined response is essential when responding to UAS incidents.
- Communications plans are coordinated to ensure a single and consistent message is released to the media and others.

Time spent in the early stages seeking endorsement of the plan and agreeing the roles and responsibilities of each stakeholder will pay considerable dividends as the mitigations are developed and eventually deployed.

Developing a C-UAS strategy and plan

The C-UAS strategy should set out:

- The details of the site to be protected and the lifetime of the site and mitigations.
- A summary of the UAS security risks and the level of risk that is acceptable to a site.
- The deliverables that are required – including, timeframes for delivery and resources needed.
- A high level statement as to the level of technical integration to be achieved.
- The approach to internal and external stakeholder engagement.

The C-UAS plan should set out:

- The detailed arrangements for stakeholder engagement.
- The roles and responsibilities of the key stakeholders.
- The outline of how technical and operational integration will be achieved with other security measures and work packages, and with other agencies (such as the police).
- Any risks/ issues/ interdependencies in relation to the project.
- The governance structure required to hold those responsible for both the delivery and operation to account.
- The detailed steps taken to prevent negligent or reckless use.
- Physical measures that can be introduced to harden critical assets.
- The arrangements made to introduce effective reporting, response and recovery of evidence to an incident.

Only if considered necessary will these documents include the elements required to deliver and operate a technical solution.

Project management considerations

The delivery of a C-UAS plan is a complex task; depending on the level of risk it may require the adaption of existing security plans and the commitment of considerable additional resources (e.g. funding, people, time and potentially the purchase of technical equipment).

Due to the complexity of delivering such a project it is recommended that a project management approach is adopted for the planning, design and delivery stages.[3]

Governance

As a result of the potential security, financial, legal, reputational and operational risks associated with UAS incidents there is a need to have clear governance in relation to the decisions that are required throughout the project and operational delivery.

Some key decisions will need to be made at the highest level of an organisation. As a level of UAS risk may be left unmitigated, it is very important that senior decision makers understand the UAS risk that remains to the organisation.

Stakeholder engagement

Stakeholder engagement is important at each stage of the development of a CUAS plan, from assessing the risk through to developing appropriate responses.

Internal stakeholders

It will be necessary to engage with those responsible for:

- Operational delivery.
- Health and Safety.
- Communications.
- Training.
- Risk management.
- Procurement.
- Delivery of legal advice.
- Human Resources (HR).
- Technology (IT).

Where there is a split in responsibility for the management of security and safety, time may need to be spent considering how these teams work together to deliver a single response.

External stakeholders

Early identification and engagement with key external stakeholders will be important. Consideration should be given to engaging with the appropriate regulators. Consider if there are working groups or fora who may already identify "best practice" and lessons learnt from similar sites within the business area the site operates within.

Local organisations whose sites are adjacent or have shared use of the site being protected are also likely to play an important part in in developing and delivering the plan.

Engagement with the police

As with all matters relating to security and policing, ***the relationships with the police are key.*** The contact may be with either the local police or those specifically tasked with providing policing to certain sites. A strong relationship is of considerable benefit and is built on understanding and compromise. It is important to identify the contacts who may be able to support the development of the plan.

[3] Further information on the development of new security projects is available on the following extranet link https://www.cpni.gov.uk/new-security-projects

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, coordinated 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 recovery of a UAV or UAV component parts, including forensic management where applicable.
- 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.

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 (described below) and enable sites to learn from how incidents have been managed.

The following are examples of some of the lessons learnt:

- Clear roles and responsibilities required between internal and external stakeholders.
- Importance of raising the awareness of all site personnel to UAS threats.
- Crisis and post incident comms to be developed, lead agency or departments agreed.
- Prioritised list of information to be gathered through reporting process.
- Fast time analysis required to inform decision making.
- Plan for a prolonged incident, consider the impact on business continuity.
- Robust testing and exercising plan required to prove the site and responders are ready.
- Need to regularly review vulnerabilities and system capabilities against evolving threats.
- Recruit visitors to the site and the local community into the reporting process.
- Understand what information could be useful for post-incident investigation, and where time permits, gather information from people reporting sightings.

02

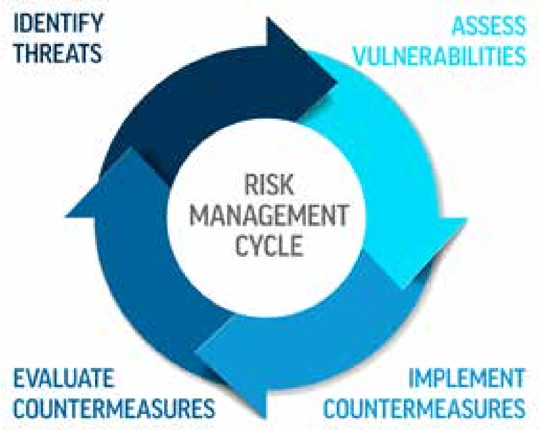
ASSESSING THE THREAT & RISK

The initial step in developing a C-UAS plan is the review of the site's existing strategic security risk assessment. This should include a high level assessment of the security risks to the site associated with UAS threats. It will involve a desktop 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. It should be reviewed on a regular basis to consider changes in UAS and C-UAS capability, trends in hostile UAS activity and site operations.

The threat is currently manifested in multiple ways. Examples of the methods that are posed to a site are: disruption, surveillance or delivery of a payload. A variety of threat actors have been seen to use these methods. The threat actors 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 threats that can be manifested at each site vary considerably. The site security risk assessment should be used to identify the threat scenarios that are likely to present the greatest risk to a site.

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

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.

Due to the range of risks that may be manifested the ownership of the risk may sit between different internal departments.

Discussions should take place between departments to provide clarity in relation to the roles and responsibilities associated with both managing and mitigating the risks and responding to incidents.

Once the strategic risk assessment has been completed, the existing overall security strategy should be reviewed and C-UAS considerations incorporated.

This process will highlight if the existing plans can be adapted or if additional mitigations are required to counter the threat of a UAS incident.

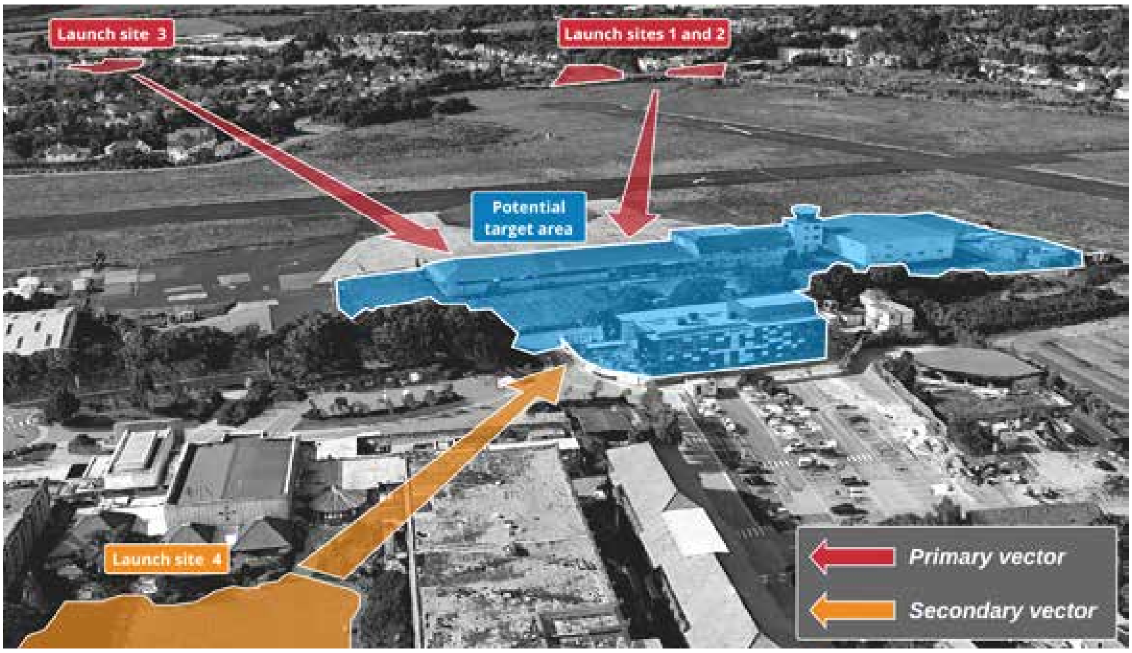
UAS vulnerability assessment

A site vulnerability assessment for UAS threats should be completed, to inform the detailed risk assessment and the C-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.

It should be noted that many sites are increasingly using UAS for a wide variety of legitimate and useful activity. This may include conducting aerial surveys or filming.

For example, some sporting and major event sites will have UAS systems being operated by both broadcasters and/or the police.



03

REDUCING NEGLIGENT AND RECKLESS USE AND DETERRING HOSTILE ACTIVITY

The vulnerability assessment should be used to consider what measures are appropriate to reduce negligent and reckless use, and to deter hostile activity. This is important to do as it assists an organisation in understanding intent and more easily identifying malicious acts, which in turn allows them to focus further protective security measures on the hostile user, thus justifying a more robust response to such incidents.

There are a range of security measures which can be employed 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 geofencing.

This section of the document provides an overview of each of these concepts and should be used to assist organisations in understanding how they may form part of their overall C-UAS plan.

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. For example, engagement may be with local schools, businesses and flying clubs.

Time will need to be spent identifying each stakeholder group and setting out in a communications plan how they should be engaged.

Security minded communications

Corporate communication resources should be developed and used by the site operators and the local police to help:

- Deter potential malicious individuals from attempting to use UAS.
- Reassure the public and the 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.

Deterrence communications can be useful in helping deter malicious individuals who are planning and researching a UAS facilitated hostile act.

The communications must actively promote an organisation or site's effective capabilities to counter UAS using all of the normal channels of communications (website, social media etc.) but without providing detail that could be useful to a hostile audience.

Showcasing, via usual communications channels, that the local communities are vigilant and reporting unusual activity can encourage further reporting. Critically, this can also help deter malicious individuals by creating a perception it's not just the police or security teams they need to be worried about as anyone, anywhere can be onto them – a very powerful effect.

It may be appropriate to erect "no drone zone" signage prohibiting the use of UAS at points of access to identified likely launch sites and nearby transport links. The signage should incorporate a unique location identifier and a reporting telephone number.

Customisable signage and artwork are available from CPNI. Consideration will need to be given to seeking the agreement of other landowners, the police or the responsible local authority for the erection of any signs at locations not under the control of the site owner. Many people do not recognise the risks posed by UAS; communications should be developed to increase the awareness of all personnel working within a site to the potential risks they pose to their site.

ZONE 32
NO DRONE ZONE
UNAUTHORISED USE OF DRONES IN THIS AREA IS STRICTLY PROHIBITED
OFFENDERS LIABLE FOR PROSECUTION

This will develop their understanding of the threat and how it may manifest itself locally, preparing them to take action should they witness an incident. Security personnel should familiarise themselves with the rules contained within the Drone Code[4] and develop a basic understanding of the offences which may be committed.

Consideration should also be given to the new regulations being introduced by the European Union Aviation Safety Agency (EASA) in relation to new rules being introduced.

[4] Additional information is available at https://dronesafe.uk/drone-code/

Such communications will increase confidence that effective measures are in place. This message may filter out to individuals considering using a UAS flight in the vicinity and so also act as a deterrence.

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.

Organisations should also put a media strategy in place. This should contain drafts of both proactive and reactive media lines, which in the event of an incursion should be aligned with both the police and Government strategies. See CPNI's information on crisis communications for more information.[5]

Airspace restrictions and geofencing

Airspace restrictions

In line with long-standing international agreements, 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 unmanned).

These may be Prohibited Areas, Restricted Areas or Danger Areas (military ranges etc). It is also possible to place a temporary restriction on airspace, either as a result of a longer term pre-planned event, or in reaction to a short notice occurrence, such as an emergency incident.

Organisations should use the CAA website and associated apps to identify which type of airspace their site is located in. This information can help sites understand the level of nuisance or reckless flights they might experience, as well as provide an indication on potential malicious intent of a pilot if flying in restricted airspace.

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 whilst flying.[6]

Geo-fencing

Geo-fencing is a virtual barrier around predefined areas of airspace. It is manufacturer specific and therefore has no effect against UAVs manufactured by someone else. It is only geo-awareness and not geo-fencing which is currently mandated at a European level, meaning that not all restricted airspace will automatically be geo-fenced.

Geo-fencing will not stop a determined malicious actor; however, it is useful for helping sites identify intent and reducing negligent and reckless use.

[5] https://www.cpni.gov.uk/system/files/documents/de/eb/Crisis_Management_for_Terrorist_Related_Events.pdf

[6] https://www.caa.co.uk/Consumers/Unmanned-aircraft/Our-role/Airspace-restrictions-for-unmanned-aircraft-and-drones/

04

PHYSICAL HARDENING

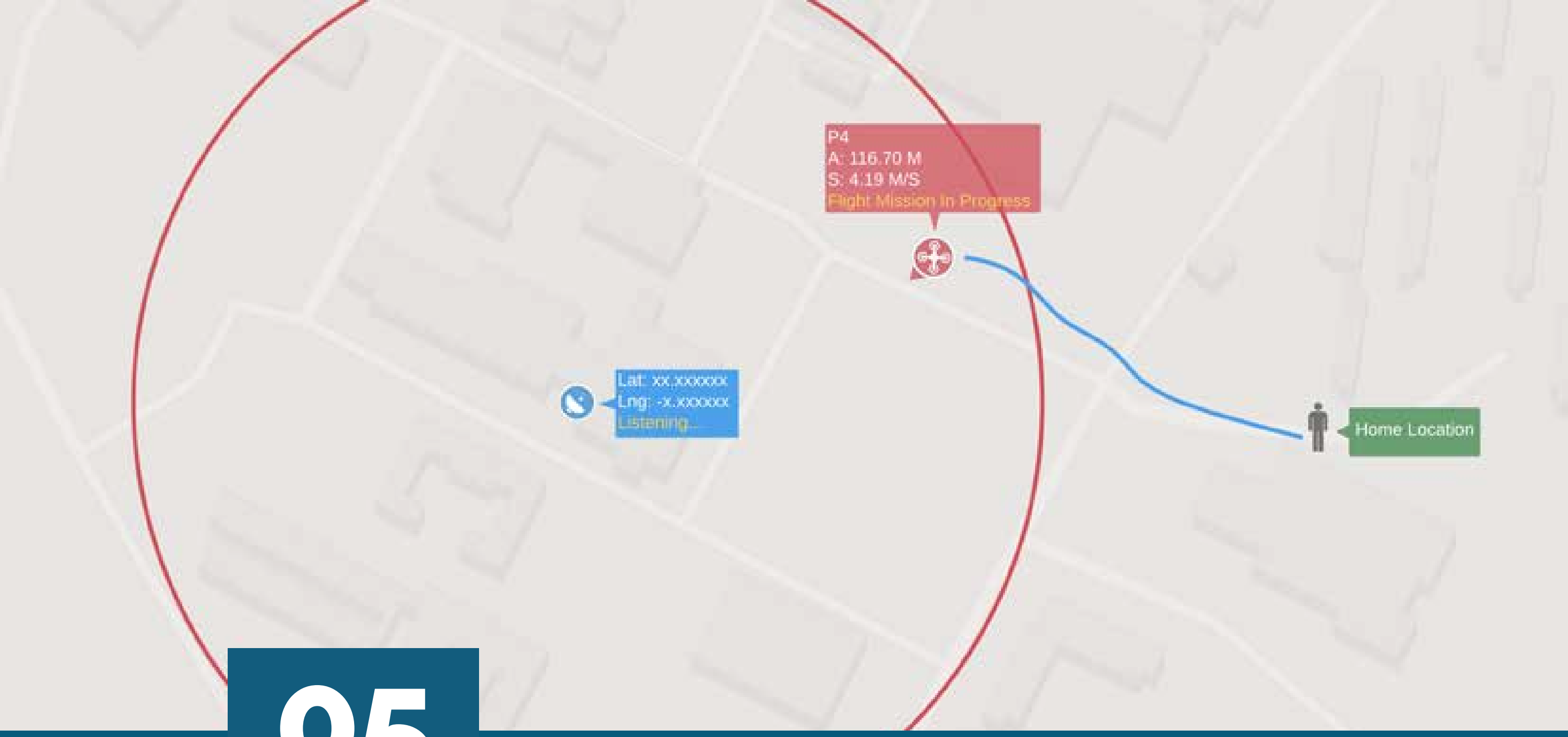
The outputs of the vulnerability assessment will determine the need to consider where and how physical hardening can be used. ***Straightforward and less expensive measures to mitigate the risk of negligent and reckless use should be adopted at the first opportunity.*** Other more complex measures such as creating physical barriers may need to be considered when a higher level of risk has been identified.

Physical security measures can be taken to help protect the asset, through for example concealment, disguise, preventing physical access or hardening. 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.

Physical Security Measures

Depending on the risks, an organisation may wish to consider:

- Designing out the vulnerability – for both new and existing sites, e.g. by moving the vulnerable assets away from the perimeter and disguising what they are.
- Cover from view – e.g. using 'cover from view' screens to make observation from outside more difficult.
- Concealing/disguising the asset.
- Protecting the asset – placing a physical barrier around it.
- Protecting sensitive information – using obscuration film, blinds or simply removing information from site.
- How existing physical security measures, such as CCTV and lighting can be used to secure the site and support the response to any incident.



05

C-UAS TECHNOLOGY SOLUTIONS

An introduction to technical counter measures.

A C-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.

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

C-UAS technical counter measures will vary on a case by case basis. The guiding principle is that 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 C-UAS technology market.

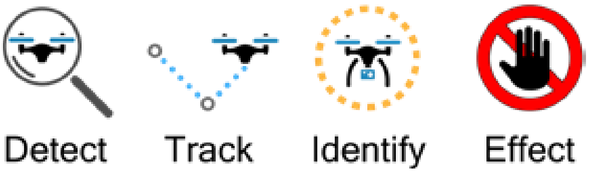
There is an ever-increasing range of different types of commercial off the shelf (COTS) C-UAS technology available.

In a rapidly expanding and developing market, it is important to understand the considerations associated with their deployment and use.

Types of C-UAS technology

Broadly speaking, C-UAS technology is comprised of:

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 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.

Developing an Operational Requirement (OR) for C-UAS technology

Once it has been established that there is a requirement for a C-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 C-UAS plan.

The OR provides a structured process for outlining and assessing security risks and identifying suitable risk mitigation options. It should result in the production of requirements to enable a proportionate solution to the issues identified.

The CPNI 'Operational Requirements' guidance document provides further information on the development of an OR. The OR will bring together all the information required to select the most appropriate C-UAS technical solution, for example:

1. Identifying the threat scenarios of greatest concern.
2. Defining what the system is intended to Detect, Track and Identify.
3. Determining when the solution is required to be in operation.
4. Setting the performance requirements of the system.
5. Agreeing the level of integration required with other safety and security systems.
6. Identifying the legislation the system needs to comply with.
7. Identifying the data security risks to be mitigated.
8. Identifying the environmental factors that must be addressed in the development of the solution.
9. Identifying the level of maintenance and support required.

Choosing C-UAS technology

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.

CPNI has therefore developed a standard to enable testing and evaluations of COTS C-UAS DTI products. The standard provides a benchmark for vendors of equipment, Government and owners/operators of sites, and a mechanism for having products independently tested.

This is a complex and rapidly changing environment. 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 should be sought from your CPNI adviser or local police Counter Terrorism Security Adviser prior to commencing a procurement.

Those responsible for the security of temporary events or crisis management situations may have differing requirements.

Importance of in situ testing

Arrangements should be made to conduct a period of **in situ** testing. This will be a period of testing that takes place at the site to be protected. The equipment should be deployed in sufficient quantity and for a period long enough to effectively test the equipment against a variety of environmental conditions and against a range of simulated threats that match the statements set out within the OR.

In situ testing should take place with the C-UAS technology fully integrated into other technical systems. The conditions for the testing should be as close as possible to those in which the equipment will finally be deployed.

Whilst this testing will identify issues directly associated with the installation of the equipment. It should also be used to identify the wider impacts and the unexpected effects, which are likely to vary, depending on the technology used.

06

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 and respond to 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 available.
- Response plans that are rapidly deployable, 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 defines how the response to any incident will be delivered, bringing together people, policies and technology.

The development and implementation of effective Standard Operating Procedures (SOPs) to assess and counter the threats posed by UAS is necessary. It is essential that good planning, training, exercising and rehearsing is used to develop and deliver effective reporting and timely responses to UAV incidents.

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 as to how the response is coordinated with the police and others.

Steady state operations

The vulnerability survey should be used to identify areas around and close to the perimeter where a UAV could be launched and consideration should be given to how security personnel and the site CCTV can be used to patrol these sites.

These same locations may again become a focus of attention if there is an incident. 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. Consideration should be given to alerting the CAA, site personnel, neighbouring sites, the public and the police as to what and when planned activity is expected, so that it does not generate unnecessary alarm or incident reports.

Encouraging reporting

Incident alerting

Detailed consideration must be given as to how 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 is available, which enables sites to identify who to call and identifies the location at which the individual is phoning in from.

Gathering accurate information

Staff should be briefed and trained in the information that they should provide if they suspect they have seen either a UAV or a GCS. 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 is assessed and a picture is 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 being triggered.

Operational response

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 / verified presence of a UAV(s) or operator(s).
- The discovery of a UAV(s) or related equipment.

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

The response plan that is developed will need to be unique to a site. It should be informed by an understanding of the UAS threats which pose the highest and most likely risk to the site.

SOPs should be developed and be available to the guardforce and other resources, that should determine their response to UAS incidents.

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 assessment processes and SOPs in place to ensure 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 C-UAS technical solution.

In making decisions the following will need to be considered:

- The available intelligence and information and its reliability/verifiability.
- Assessment of the threat.
- The available options.
- The 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 considering how the following tasks will be delivered:

- Taking decisions on how to respond to the threat.
- Considering the implications for current site operations and the safety of the people on the site.
- Deployment of security guardforce and others.
- Engagement with police and other external stakeholders.
- Crisis communications, including appropriate messaging to staff and/or the public.

Recovering suspect UAS

The response plan needs to incorporate what should happen if a UAS is recovered or a report received of a grounded UAV/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.

Post-incident review

In the aftermath of an incident, the information gathered may be used to support post incident learning and the continued investigation into any offences that may have taken place.

Once the incident has concluded a post incident report should be prepared. This will support the investigation and identify lessons learnt that may be used to improve the response, including for example, learning from the reporting process and updating the site vulnerability assessment.

C-UAS Exercise Plan

Making sure plans are operationally effective

The response plan should be built on the operational and technical resources that are available to respond to the incident.

Whenever possible the plan will be based and built on the same principles and processes as other existing site response plans and the overarching site security plan.

Planning must not be done in isolation and should consider the involvement of a range of key internal and external stakeholders.

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. An exercise plan should be created that will set out how to assure that:

- The C-UAS response plan and reporting processes have been validated and any gaps identified.
- Roles and responsibilities of internal and external stakeholders have been defined and tested against a range of reasonably foreseeable scenarios.
- Staff are appropriately trained and briefed on how to respond during a UAS incident.
- The concept and implications of deploying specific technical security equipment is understood prior to procurement and use.
- Technical equipment has been robustly tested prior to go live.

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

Concept of Operations

A Concept of Operations (CONOPS) should be developed that sets out the end to end response to a UAS incident.

It will provide a bridge between any technical equipment deployed, the operational response and the relevant security and safety policies.

It should document how the operators in the control room will interact with the equipment and use the information obtained from it to inform the decisions that will need to be made.

At every planning stage consideration should be given as to how the response and CONOPS can be developed and improved.

07

REVIEW

Implementation plan review

The impact that both negligent/reckless use and hostile UAS activity can have on sites is clear. It is therefore necessary to spend time identifying the risks to the site and considering what mitigations could be introduced. This is likely to require a carefully considered and detailed approach to planning the solution. This guidance has been formulated to ensure that the mitigations that are developed are all effectively integrated.

This document provides an introduction to the major steps that are required to mitigate the risks of unauthorised and hostile UAS activity through the development of a C-UAS plan. In summary, the steps are as follows:

1. Identify the components of a C-UAS strategy and plan
2. Understand the risks posed by UAS and conduct a site vulnerability assessment
3. Determine what can be done to reduce reckless/negligent use and deter hostiles
4. Identify the role that physical hardening can play
5. Ascertain the appropriateness of deploying C-UAS technology
6. Develop reporting and response procedures
7. Review the C-UAS strategy and plan

Annex A contains a list of the key planning tasks and considerations associated with each stage. It provides a checklist to assist organisations completing the necessary tasks to develop the strategy and plan.

Ongoing review

Once a plan has been implemented and tested to provide confidence that it works it should be regularly reviewed. An ongoing review process will need to be developed so that it covers both the operational deployment of the plans and periodic strategic reviews to make certain that the plan continues to mitigate the developing risk (updated information will be available from your local police contact). In addition, after any incident involving the intrusion or attempted intrusion of a UAV to the site there should be a review to establish what lessons can be learnt and how the plan could be improved.

Annex A: C-UAS planning checklist

The development of a C-UAS protective security solution involves detailed planning. This annex provides a list of the key planning tasks and considerations.

Planning

□ Consider how the existing site security strategy and security risk assessment address UAS threats

□ Identify resources to complete tasks

□ Establish governance: which individual at the highest level of your organisation is accountable

□ Identify and engage with internal stakeholders

□ Engage with the Emergency Services

□ Identify local organisations and communities

Assessing the threat and risk

□ Complete site vulnerability assessment

□ Identify key assets

□ Identify threat scenarios

Reducing negligent and reckless use

□ Develop a community engagement plan

□ Prepare communications plan

□ Consider the use of signage

□ Consider airspace restrictions and geo fencing

Physical hardening

□ Identify how physical hardening can be used to protect the site

□ Identify what can be done to make launch sites adjacent to the site less appealing to use

□ Develop a plan to introduce physical hardening

C-UAS technology

□ Identify if the site has a requirement for C-UAS technical counter measures

□ If yes, develop an operational requirement for C-UAS technology and use to inform the selection of appropriate solutions

Reporting and response

□ Review the role of the SCR in the response to a UAS incident

□ Review roles and responsibilities of all key resources and decision-makers involved in responding to an incident

□ Develop reporting processes to ensure accurate and timely reporting

□ Develop a response plan that covers different types of potential incidents and considers the implications for activities and people at their site

□ Develop SOPs

□ Develop a C-UAS exercise plan

□ Consider the training requirement

□ Develop CONOPS