QINETIQ

Application Note:

Protection of Airspace Surrounding Critical National Infrastructure Sites

Phil Cork, QinetiQ December 2021

QINETIQ/CF/CM/CS2100094

In this application note we discuss the need to provide physical security at Critical National Infrastructure (CNI) sites, and the relative lack of capability to protect the airspace above and surrounding them. You'll learn about the relative strengths and weaknesses of airborne threat technologies for the defence of CNI sites, and through the use of an 'OODA loop' methodology, how you can develop a more holistic capability for site protection.

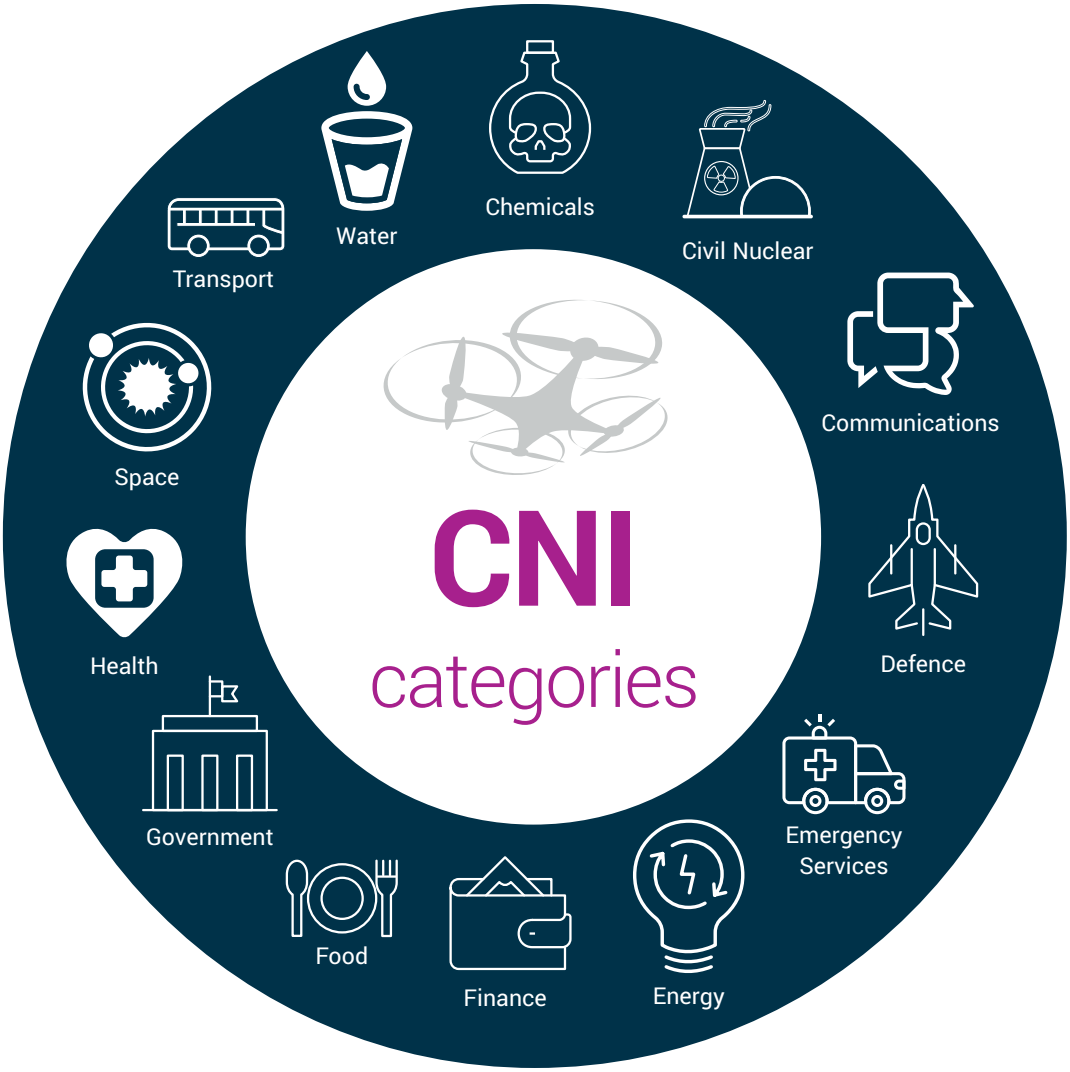


Figure 1: Graphic showing the 13 sectors that Critical National Infrastructure is comprised of.

A solution, QinetiQ's 'Obsidian', is presented for the automatic verification of airborne threats, helping you better mitigate the impact of a perceived or real airborne incursion to your site.

Current Approaches to Protecting CNI

Sites and installations which comprise 'Critical National Infrastructure (CNI)' conventionally require, as a minimum, comprehensive Physical and Cyber security systems, which protect the installation, its staff and visitors, and the sensitive data and information relating to its operation.

A typical installation is shown below:

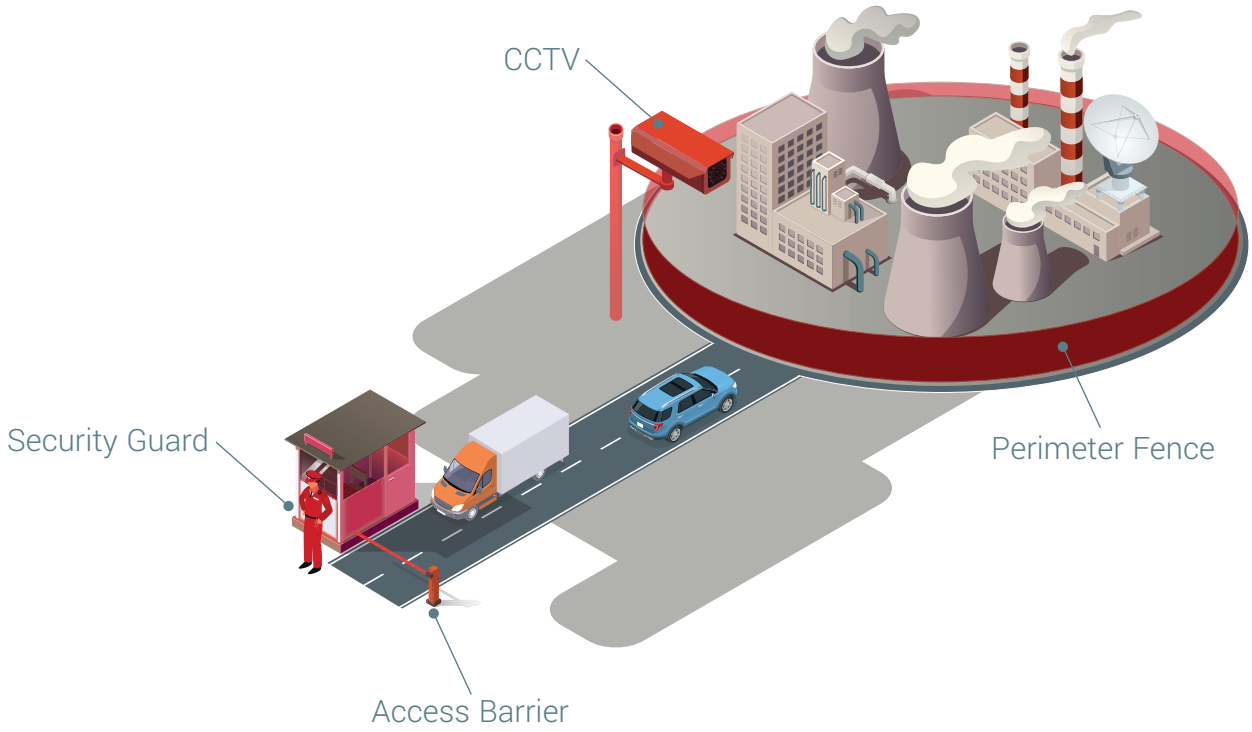


Figure 2: Representation of a site with a vulnerability from the air. Items in red are traditional monitoring/defence installations.

As can be seen, physical security systems comprise manned gated site entry systems, security fencing with potential anti-scale treatment (electrified fencing and/or barbed wire), and closed-circuit television systems, increasingly Internet Protocol (IP) – based, which allow site security staff to view the surrounding area and monitor suspicious activity and/or attempted entry from a central operations location.

In addition are both remote and physical cyber security attacks that aim to compromise an organisation's digital infrastructure (not shown above). A Security Operations Centre detects, investigates and analyses any incidents promptly, with alerts being raised and immediate action being taken to minimise the risk of operational disruption from a potential security breach. Additionally, exercises such as penetration testing and red teaming allow you to simulate the latest targeted attack methods used by real world adversaries to strengthen your defensive teams and identify critical vulnerabilities in your security posture.

These systems, and the commercial organisations that provide them, have matured over decades of operation, and with relatively few exceptions successfully provide 'ground level' physical resilience to CNI operation, and a broadly compressive level of Cyber Security.

Unmitigated threats from above

Consideration of the above diagram and accompanying description reveals a potentially glaring omission, the airspace above, surrounding and approaching the site.

Recent well publicised events such as the Drone incident at London Gatwick Airport (LGW)[1], the landing of a drone on a UK Navy Aircraft Carrier[2], and a 'swarm of drones invading' Palo Verde Nuclear Power Plant[3] demonstrate how easily CNI airspace may be compromised, leading to significant disruption, loss of revenue potentially into the tens or hundreds of £m, and potentially loss of life.

Drones however don't represent the only threat from the air. Microlight aircraft such as that shown below are available online for as little as a few thousand US$ and could be used to gain access to CNI from above. Also, as evidenced during the recent Euro 2020 championship, parachutists utilised by activists are also capable of causing disruption and injury[4].

Also, this September will mark the 20th anniversary of 9/11, where commercial jetliners were used in the largest scale air attack on 'critical infrastructure' outside of war.

The proliferation of low-cost air vehicles as a means of causing disruption, harm, and threat to operations and life poses an increasing threat to CNI installations, which typically approach physical security as a 'ground level' issue.

1. 'Sustained' drone attack closed Gatwick, airport says - BBC News
2. Tiny drone lands on Queen Elizabeth aircraft carrier - BBC News
3. 'Drone Swarm' Invaded Palo Verde Nuclear Power Plant Last September — Twice (forbes.com)
4. Euro2020: Terrifying moment a Greenpeace protester parachutes onto pitch before Germany vs France - YouTube

Risk to operations

The decision loop below is a typical counter-drone OODA loop – Observe, Orient, Decide, and Act for the example of a drone threat. In order to be resilient to the threat of drones (or other airborne threats), it is important to have considered the phases of the OODA loop and have developed robust procedures and processes for security staff to follow to properly protect operations.

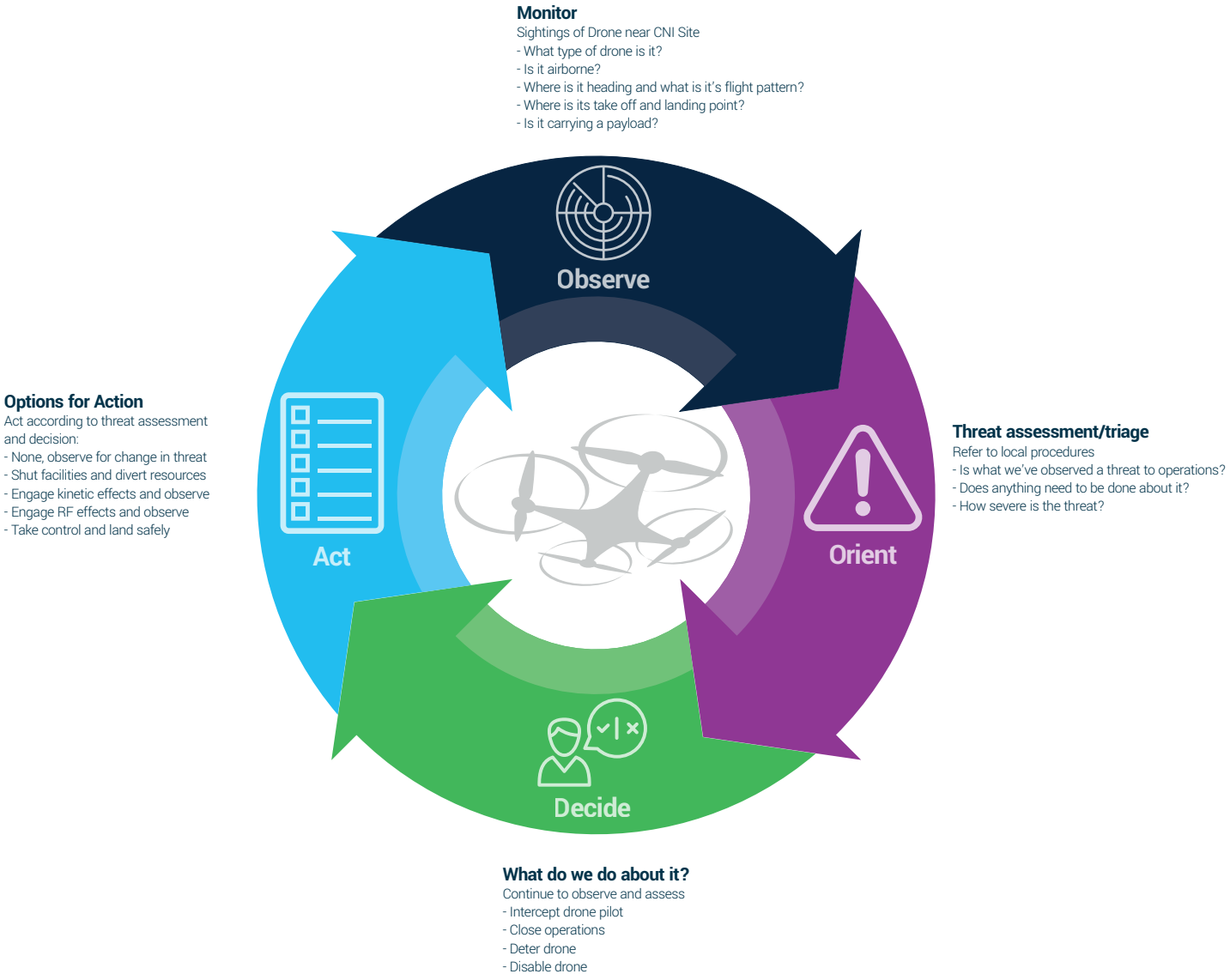


Figure 3: Observe, Orient, Decide and Act decision loop

In the absence of an airspace surveillance system, the 'Observe' phase is likely to consist of the following:

- Informal reports (potentially numerous) of airborne threat – telephone, security staff over radio, staff reports
- Attempts to confirm presence of threat using conventional systems – security staff searching for threat, utilising CCTV cameras outside of their intended use case, staff being put on alert to look out for the threat
- Concern for site operations and safety, potentially undue
- Inability to characterise/rank threat, therefore risk to operations unknown

The above is unlikely to lead to complete situational awareness, at least within the time taken for a threat to cause damage, therefore in the absence of sufficient information to fully inform the 'Orient' and 'Decide' phases, action is most likely to be taken to minimise risk.

This could result in evacuation of staff from sensitive areas of site, lockdown of personnel, shutting down of valuable operational equipment, and in the example of LGW, closing an airport to departing and arriving air traffic and diverting all inbound flights elsewhere.

Perhaps more importantly, without sufficient situational awareness and a means of clarifying that the threat has been mitigated or is no longer present, security personnel lack the information with which to declare all clear, and resume operations.

The damage from an event such as the above is clear:

- Initial confusion leads to a lack of risk analysis and likely preoccupation of a number of staff, who may have been intentionally diverted to allow threat action elsewhere
- The inability to properly perform threat assessment leads to overreaction and potentially significant financial and reputational loss, as well as damage to equipment or health from the threat itself
- The lack of situational awareness prevents operations from resuming in a timely manner, and is a threat to operational resilience

Airspace situational awareness solution space

The above highlights the risk to CNI operations due to the lack of airspace situational awareness and/or defence systems. The proliferation of low-cost devices capable of presenting a threat to operations, security, or life further exacerbates the problem. The risk profile for typical CNI installations therefore has to be considered to have increased significantly in the last decade.

How best to mitigate this risk therefore? Firstly considering the nature of the airborne threat, we can consider that it is likely to exhibit one or more of the following characteristics, which may render it difficult to detect:

- Small, such as a drone,
- Slow moving or stationary
- Acoustically Silent – not utilising mechanical propulsion (such as a parachute)
- Radio Frequency (RF) silent – not communicating
- Approaching from above, not 'flying' in conventionally
- Uncooperative – not transponding or communicating

The most suitable detect and track technology for such targets is radar, which is target agnostic, and can be engineered to provide reliable detection and tracking of such non-cooperative targets. Radar provides the most threat-agnostic airborne target detect and track technology[5], and isn't reliant on Radio Frequency (RF) libraries (used to recognise communications). When extended to the above non-drone threats, radar also provides the capability to detect and track non-transmitting threats, which would elude RF sensors.

However, not all radar are suitable to the task, let us consider some typical candidates:

Air traffic radar

On the face of it, air traffic radar would appear an ideal choice for CNI airspace security, however for a variety of reasons it's wholly unsuitable. Air traffic management systems typically employ a pair of radar systems to provide detection and tracking of aircraft on approach and departure from an airport. The primary radar utilises a narrow vertical beam to accurately measure range and bearing to an aircraft, and the secondary radar interrogates aircraft transponder systems to 'read' aircraft altitude, callsign and other information and overlay this with the 2D position information from the primary radar. In this manner, this pair of radar systems is able to detect, track and identify cooperative targets in the vicinity of the airport.

However, such systems are large, expensive, and arguably over-engineered for the CNI threat, and in the absence of large cooperative targets, are reduced to 2D detect and track only and are either unlikely to detect small targets, or will dismiss them as birds.

5. QinetiQ - Download the counter drone whitepapers

Battlefield surveillance radar

Battlefield surveillance radars are designed to provide detection of moving ground targets, e.g. personnel, and vehicles such as tanks or armoured personnel carriers. They typically employ Doppler techniques to distinguish moving targets from background clutter, and can be engineered to provide long range (several km) detection and tracking of small objects. However, they almost exclusively provide 2D information, measuring range and bearing only (ground targets are just that!), and are therefore not capable of proving accurate position information for air targets.

The counter-drone market has seen a proliferation of Battlefield Surveillance radar re-purposed for airborne drone detection. Typically utilised in first-generation counter-drone systems, they are not capable of automatically setting on cameras or other system sensors/effectors as they lack height measurement.

Marine radar

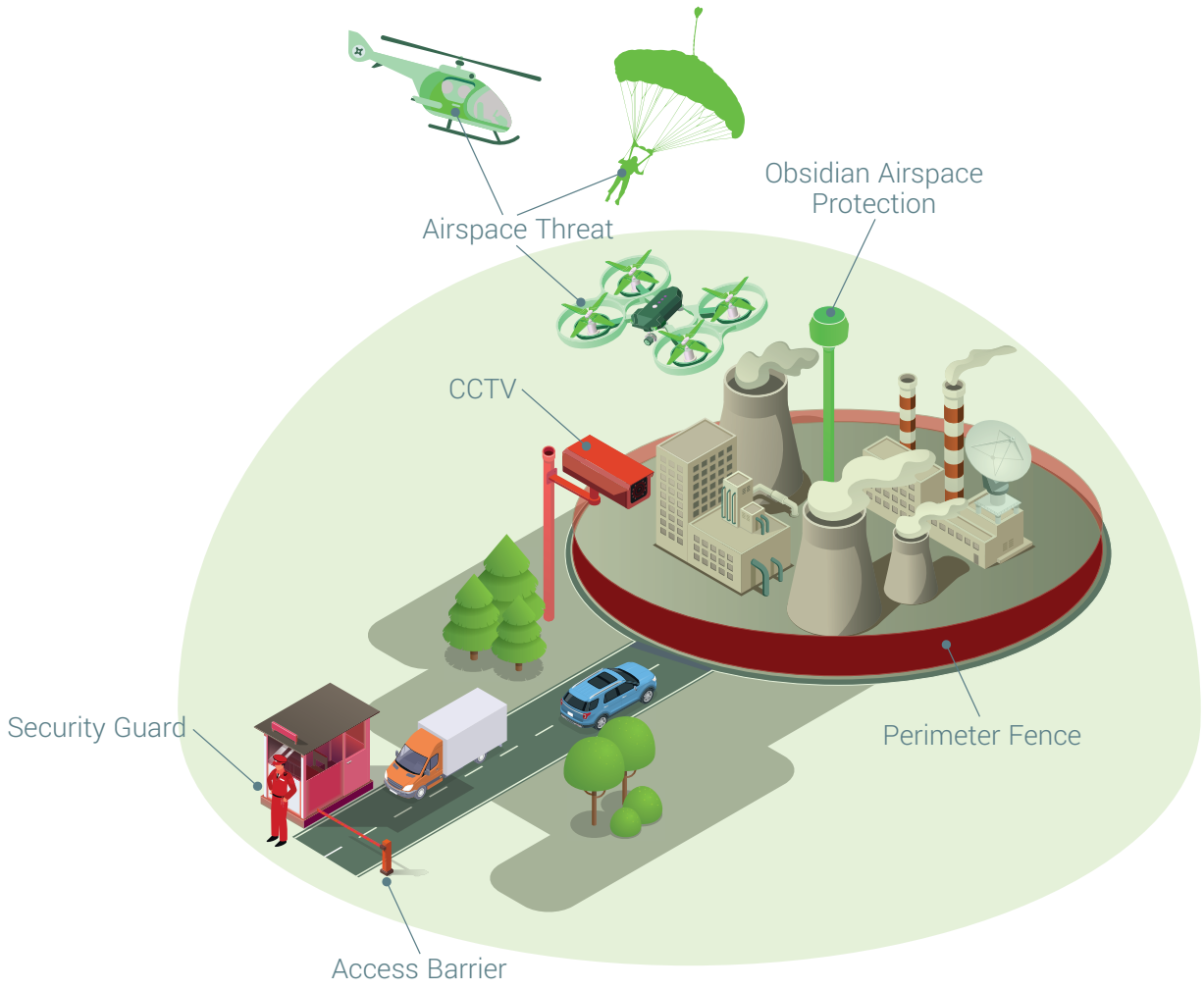
Marine radar may be purchased relatively cheaply and would appear to provide some utility for detection and tracking of relatively small objects. However, for similar reasons as stated above, marine radar utilises a vertical fan beam to measure accurate bearing and range, and assumes that all targets are at sea level. It is therefore unable to provide accurate 3D target measurement for airborne targets.

Air Defence radar

Air defence radar is designed to provide long range, accurate, 3D measurement of target position in order to set-on 'hard kill' effects (missiles) to disable enemy aircraft. As such, it would appear ideal for protection of CNI airspace. However, Air Defence radar systems are prohibitively expensive, and are designed for far greater range than is required for CNI site protection and therefore are unlikely to perform at short range, and against small targets such as drones or parachutists. They may also not provide cover immediately above their location as they're typically scanning the airspace several 10's of km from their location.

Obsidian: QinetiQ's Solution for CNI airspace protection

Recognising the growing threat to CNI airspace from modern threats such as commercial off-the-shelf drones, and activists utilising micro-light aircraft or other improvised air vehicles, and that conventional radar systems would struggle to provide capability to detect them, QinetiQ began development of a novel radar system in 2015. This radar system, Obsidian, was designed specifically for detection and tracking of small, non-cooperative, airborne threats in the airspace around a critical or sensitive location.



Uniquely in its class of radar, QinetiQ's Obsidian Radar provides full elevation coverage of +80° to -10°, and 180° in Azimuth, and therefore when placed back to back, a pair of radars provide a 'dome' of airspace monitoring around sensitive installations at CNI sites, or across a full CNI site.

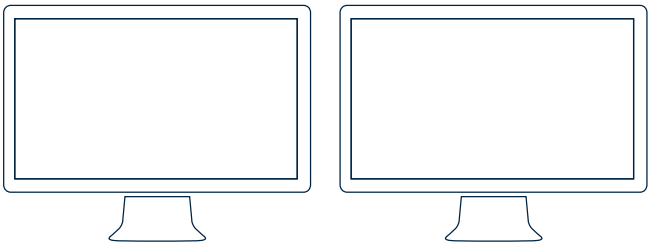
Such an installation, not possible with conventional radar systems, is capable of not only scanning above the site boundary for incoming airborne threats from long range, but can also provide detection and tracking of targets approaching from directly above, such as would be the case for a parachute or items dropped from overhead aircraft or drone.

QinetiQ ‘Obsidian’ solutions

QinetiQ’s Obsidian system provides a turnkey solution for CNI airspace protection. Engineered using an open architecture Operator Interface and control system proven in Afghanistan, and incorporating QinetiQ’s unique Obsidian radar augmented with 3rd party cameras and other sensors as appropriate, we are able to configure systems for a variety of CNI sites of varying size and criticality.

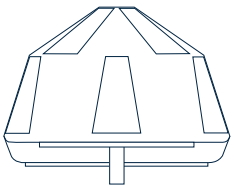
Automated Command and Control system

Open architecture & MOD compliant

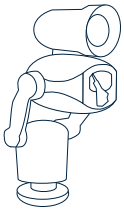


Systems Engineering

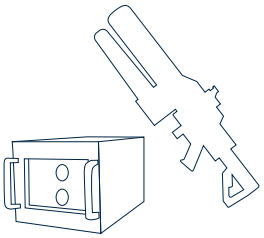
Radar systems | Image processing | RF Counter measures | Directed energy | Electronic systems



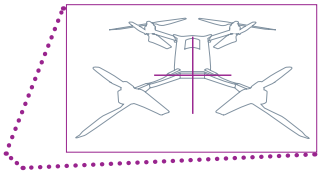
Purpose built drone detection radar



Commercial video camera systems



3rd party drone defeat systems



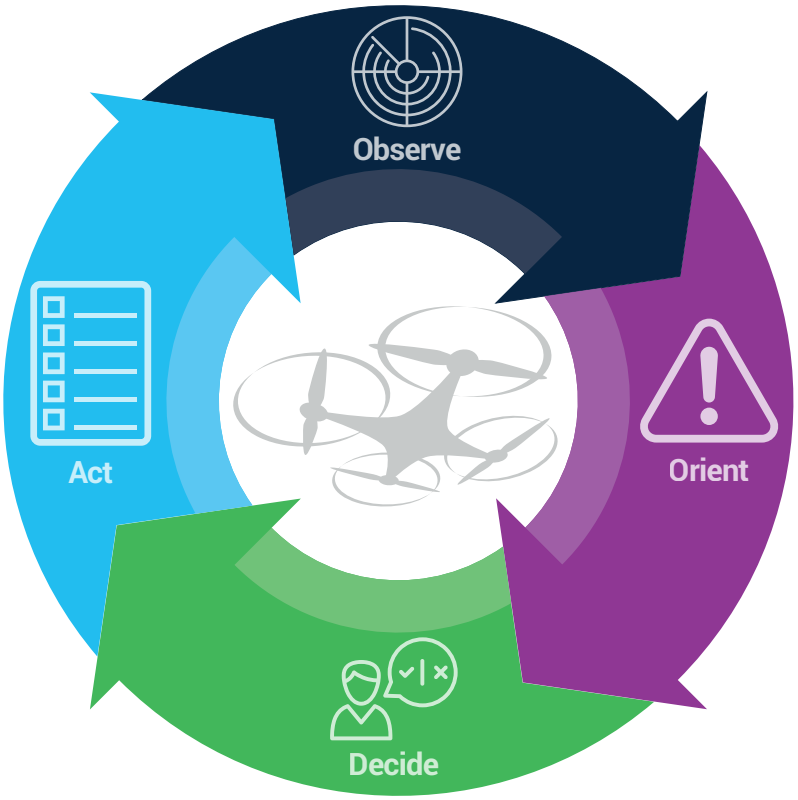
QinetiQ drone defeat systems

Obsidian is designed to be utilised in a busy operations room, and is therefore able to operate un-manned – only drawing operator attention on alarm when user-defined threats are detected. Obsidian Radar systems provide comprehensive airspace coverage, and automatically slew camera systems to provide visual threat confirmation to Operators following an alarm. Obsidian may also be augmented with additional surveillance systems such as perimeter radar systems, supplementary camera systems, or countermeasures such as RF jamming systems for drones.

Obsidian as an effective CNI airspace protection measure

Considering again the OODA loop for a CNI site, but with an Obsidian system installed and its command and control suite displayed in the site control room.

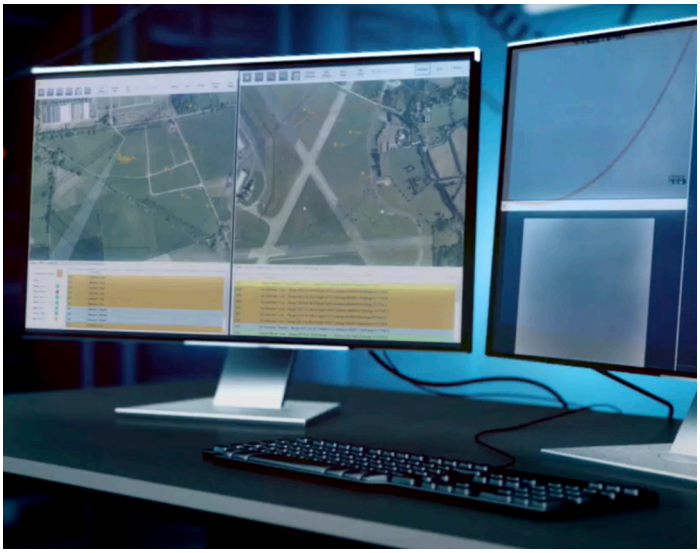
Monitor
Sightings of Drone near CNI Site
- What type of drone is it?
- Is it airborne?
- Where is it heading and what is it's flight pattern?
- Where is its take off and landing point?
- Is it carrying a payload?



Options for Action
Act according to threat assessment and decision:
- None, observe for change in threat
- Shut facilities and divert resources
- Engage kinetic effects and observe
- Engage RF effects and observe
- Take control and land safely

Threat assessment/triage
Refer to local procedures
- Is what we've observed a threat to operations?
- Does anything need to be done about it?
- How severe is the threat?

What do we do about it?
Continue to observe and assess
- Intercept drone pilot
- Close operations
- Deter drone
- Disable drone



Observe

Critically, Obsidian automatically provides highly accurate and timely Situational Awareness, showing the tracks of all air targets as they're detected, and likely before they've been spotted and a call/radio has alerted security staff.

Once a target has been assessed to be a potential threat, Obsidian slews the system camera onto the threat and sounds an alarm – altering security staff to the system user interface:

Orient

Security operators can then assess the threat through the track information (is the target on a trajectory to the site, is it in the path of aircraft etc.), the video feed and supplemental RF sensors (which may be able to determine drone type.

Decide

Referring to local procedures, the appropriate action can then be directed by the security team, including continuing to Observe, Orient and Decide whilst the threat isn't critical, preserving operations.

Act

With a complete and up to date Situational Awareness, accurate threat assessment, and thereby informed decision making, security teams can then take proportionate and appropriate actions, which balance the threat to operations with the need to maintain them.

Summary

While conventional site security solutions have evolved into mature, resilient ground-level physical security and cyber security systems, a growing threat is manifesting in the air domain, resulting in a vulnerability to airborne assault.

Recent well-publicised examples have demonstrated this vulnerability, and the financial and reputational cost can be measured in the tens of £millions.

Without an airborne security system and accompanying processes and procedures, CNI organisations are exposed to confusion, inability to properly assess threats and risk to operations, and are likely to react disproportionately; either underestimating the threat – leading to damage or loss of life, or overestimating the threat – leading to loss of income and/or reputational damage.

Key to a resilient airspace security system is accurate and timely situational awareness, without which a proper risk assessment cannot be performed. QinetiQ have developed a solution to CNI site airspace protection, Obsidian, which is designed to provide high levels of automated airspace situational awareness, supporting resilient operational through accurate and timely airborne threat assessment and tracking. Obsidian also allows, subject to legislative approval, set-on of effectors for defeat of commercial drones.

QinetiQ recognise that resilient systems typically require layering of technologies to achieve the best on-site performance, and are able to work directly with CNI operators, and/or co-develop solutions with global primes, OEMs, or SMEs.

QINETIQ

For further information please contact:

Cody Technology Park
Ively Road, Farnborough
Hampshire, GU14 0LX
United Kingdom

+44 (0)1252 392000
ObsidianInfo@qinetiq.com
www.QinetiQ.com

QINETIQ/21/04394