HM Government

Behavioural detection

Best practice, guidance and advice

CPNI
Centre for the Protection of National Infrastructure

Department for Transport

[dstl]
The Science Inside

NaCTSO

Executive Summary

The term 'behavioural detection' refers to a method of detecting individuals with hostile intentions by observing their behaviours and activities. This guidance is written by behavioural detection experts from across government, and has been informed by consultations with key stakeholders and other specialists as well as by research and other literature.

The purpose of this document is to inform those considering the use of behavioural detection and to provide specific advice for various stakeholders. It can help those needing to better understand (a) different behavioural detection approaches, (b) the strengths and weaknesses of these, and (c) how to choose and apply behavioural detection methods to specific environments to maximise the security of a location and its people.

As such, this guidance is designed to help both policy makers in government and industry who are responsible for advising and/or mandating security processes and measures, and those on the frontline responsible for ensuring security, such as security managers across a range of different sites.

This guidance provides information on:

- The role of behavioural detection within protective security, plus the pros and cons and other matters that should be considered before deciding to include the use of behavioural detection as a security measure.
- How behavioural detection works, and the need to set up and adapt the environment to help elicit behaviours of concern whenever possible.
- The vital importance of rapidly and effectively resolving suspicions that result from behavioural detection.
- Types of behavioural detection – from specifically trained personnel to public campaigns that encourage vigilance and reporting of suspicious activity.
- Matters to consider before procuring or instigating a behavioural detection capability.
- Measures of effectiveness and evaluation of training, technology and equipment.

Executive Summary

When incorporated with other security measures, behavioural detection can be a powerful tool that can be implemented in a range of environments, as part of a systematic approach to disrupt criminals and terrorists carrying out activities that aim to cause harm to others. This overall approach to disruption may include (i) detecting individuals (e.g. whilst conducting hostile reconnaissance), (ii) deterring thieves (e.g. from targeting a venue), and (iii) denying different types of criminals (e.g. access to information they need to plan an illegal activity)[1].

Behavioural detection can contribute to this disruption. However, it is vital to note that behavioural detection:

- Is not a panacea in protective security; it should be seen as part of a systematic approach to the security of a site – detection is just one aspect of this.
- Can be expensive to implement and difficult to retain as a capability, especially if staff turnover is generally high, unless there is a rolling training programme.
- Requires staff to use their skills regularly, to maintain competence.
- Requires a clear process in place for staff to rapidly, effectively and fairly resolve suspicions about any persons of concern.
- Requires on-going monitoring and evaluation to ensure it is effective and does not have or develop inherent biases that can skew outcomes (e.g. whereby individuals are prejudiced against because of their gender, race or mental health issues).

1. These are the '3Ds' of CPNI's disruption model. See https://www.cpni.gov.uk/disrupting-hostile-reconnaissance

Executive Summary

It is important to note that if trained personnel are expected to conduct behavioural detection but also other duties at the same time, this will limit the effectiveness of the capability. Moreover, the potential of behavioural detection to be effective is significantly impacted by the number of trained staff on duty, the area that they are covering, and other elements of the environment.

This guidance paper sets out key points to consider regarding the use of behavioural detection to contribute to the security of different environments. It outlines when, where, why and how behavioural detection may be effective or fail, and critically, what to consider when contemplating the use of behavioural detection. The guidance can be used to assist those responsible for the security of different environments, to ensure that any application of behavioural detection meets requirements and is successful. It should therefore be read and used by those responsible for security at strategic, operational and tactical levels. Doing so can lead to a shared understanding of behavioural detection in terms of both its strengths and its weaknesses, ensure that misunderstandings and myths are dispelled, and that the capability is implemented in an appropriate, proportionate and effective way.

Behavioural detection capability has the potential to detect, deter and deny hostiles from operating in a range of contexts and environments. However, it is important to note that:

Behavioural detection should only be deployed as part of an integrated system to ensure that it complements and is complemented by other security measures.

It is vital that the set-up of the environment is conducive to and organised in a way that can maximise the potential success of behavioural detection, and that training provides skills and techniques that are evidence-based and tailored for different audiences.

Those considering the procurement and deployment of behavioural detection capability should ensure that they do so in an appropriate and proportionate way and have the resources to do so.

Section 1: Introduction and background

1 Introduction and background

1.1 Purpose of this guidance

This guidance has been written by behavioural detection experts from across government, and has been informed by consultations with key stakeholders and other specialists as well as by research and other literature[2].

The purpose is to inform those considering the use of behavioural detection and to provide specific advice for government and businesses.

The guidance sets out key points to consider regarding the use of behavioural detection to contribute to the security of different environments. The aim is to demonstrate when, where, why and how behavioural detection may be effective or fail, and critically, what to consider when contemplating the use of behavioural detection.

1.2 Who this guidance is for

The guidance has been written for various stakeholders; primarily those needing to better understand different behavioural detection approaches, the strengths and weaknesses of these, and how to choose and apply behavioural detection methods to specific environments to maximise the security of a location and its people.

As such, this document is designed to help both policy makers in government and industry who are responsible for advising and/or mandating security processes and measures, and those on the frontline responsible for ensuring security, such as security managers across a range of different sites.

1.3 What is behavioural detection?

In the current guidance we use the term 'behavioural detection' to mean a method of detecting individuals with hostile intentions by observing their behaviours and activities[3]. Other terms are sometimes used interchangeably (e.g. 'behaviour awareness', 'behaviour analysis') but behavioural detection is our preferred term.

This guidance frequently refers to 'hostiles' or 'hostile individuals', meaning a range of individuals who are at a site for malicious reasons. This includes pickpockets and shoplifters, and others who are at a site to gather information and conduct other actions ('hostile reconnaissance') as part of plans to conduct a terrorist attack.

2. Senior security staff in major UK transport hubs and other specialists were consulted, and a systematic review of the literature and online resources, websites etc. was conducted.

3. It is important to note that behavioural detection can also provide a strong deterrent effect.

1 Introduction and background

Key definitions

HOSTILE

"A person who wants to attack or disrupt an organisation for profit or to make a political or ideological point"

HOSTILE RECONNAISSANCE

"The purposeful observation with the intention of collecting information to inform the planning of a hostile act against a specific target"

HOSTILE INTENT

"What a hostile wants to achieve to meet their overall aims"

Advocates of behavioural detection suggest that in the right environment:

- Some people with hostile intentions can exhibit overt, observable 'cues';
- Security staff (and others, including the public) can be taught to identify these cues, and as such can detect individuals with hostile intentions;
- Behavioural detection can be used to deter hostiles and to reassure the public.

It is also important to note that behavioural detection may lead to staff noticing and being able to help members of the public who may be distressed and/or need help. For example, people may be behaving unusually compared to others around them, because they are lost, have mental health issues or are having suicidal thoughts, or because they need help for other reasons.

When incorporated with other security measures, behavioural detection can be a powerful tool that can be implemented in a range of environments, as part of a systematic approach to disrupt criminals and terrorists carrying out activities that aim to cause harm to others. This overall approach to disruption may include **detecting** individuals whilst they are conducting hostile reconnaissance, **deterring** thieves from targeting a venue and **denying** criminals access to information they need to plan an illegal activity.
These are the '3Ds' of CPNI's disruption model (see Figure 1 on Page 10). Behavioural detection can contribute to this disruption.

1 Introduction and background

However, it is vital to note that behavioural detection:

- Is not a panacea in protective security; it should be part of a systematic approach to the security of a site – detection is just one aspect of this.
- Can be expensive to implement and difficult to retain as a capability if staff turnover is generally high, unless there is a rolling training programme.
- Requires staff to use their skills regularly, to maintain competence.
- Requires a clear process in place for staff to rapidly, effectively and fairly resolve suspicions about any persons of concern.
- Requires on-going monitoring and evaluation to ensure it is effective and does not have or develop inherent biases that can skew outcomes (e.g. whereby individuals are prejudiced against because of their gender, race or mental health issues).
- Should only be considered as a mitigation on completion of a full security risk assessment

It is also important to note that if trained personnel are expected to conduct behavioural detection as well as other duties at the same time – this will limit the effectiveness of the capability. Moreover, the potential of behavioural detection to be effective is significantly impacted by the number of staff on duty who are trained, the area that they are covering, and other elements of the environment. For example, how busy or quiet it is or how the area is set up and whether there are measures in place that act as a stimulus to elicit behaviours from those with hostile intent or conducting hostile activities.

1.4 What this guidance contains

This guidance provides the policy maker and security professional with an understanding of:

- The role of behavioural detection within protective security, plus the pertinent considerations before deciding to include the use of behavioural detection as a security measure.
- How behavioural detection works, and the need to set up and adapt the environment to help elicit behaviours of concern whenever possible.
- The vital importance of rapidly and effectively resolving suspicions that result from behavioural detection.
- Types of behavioural detection – from specifically trained personnel to public campaigns that encourage vigilance and reporting of suspicious activity.
- A checklist of matters to consider before procuring or instigating a behavioural detection capability.

Section 2:
The role of behavioural detection in protective security

Often behavioural detection is seen by security managers as a desirable, additional layer to protective security. It is expected and perceived to enhance the detection capability of a site and potentially act as way of disrupting a wide range of criminality, for example through the deterrence or detection of hostile individuals.

Indeed, this can be the case for a well-trained behavioural detection capability, but, as this guidance will show, **behavioural detection is a specialist skill that requires training, frequent use and continuous evaluation, and should be used strategically in a proportionate and effective way**.

Most organisations tend to have a limited behavioural detection capability, depending on the size of the venue and available resources. It is rarely possible for a behavioural detection capability to cover all parts of a site at all times. Therefore, to be as effective as possible, it needs to be deployed across key areas of a site (e.g. where hostile activity is most likely), at specific times (e.g. when hostile activity is most likely).

It is imperative that a location or organisation is not wholly reliant on specialist behavioural detection capability to detect hostile individuals. Every site should use the entirety of its people and other resources (e.g. staff and the public, security officers and CCTV) to full effect, with or without a dedicated behavioural detection capability.

How to achieve this is covered in Section 2.2.

2 The role of behavioural detection in protective security

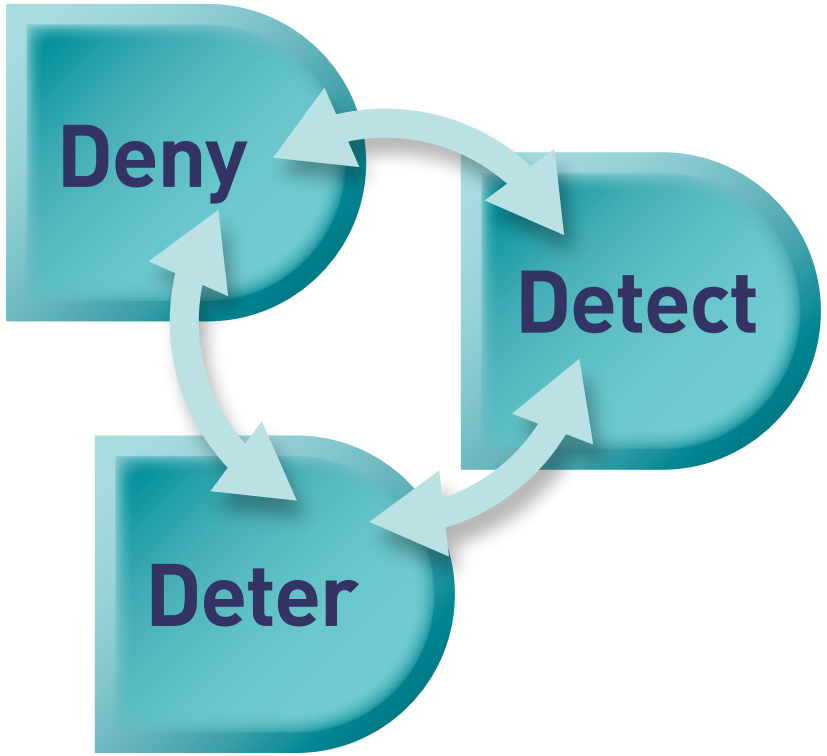
2.1 The 3Ds of disruption

Behavioural detection is not the only approach available to a site to disrupt those with malicious intent. There are other methods of disruption that are practical and relatively easy to implement and sustain, instead of or alongside a specialist behavioural detection capability.

For example, use of corporate communications to promote capabilities and using staff in customer engagement roles to have a stronger security function by attending to and engaging with suspicious individuals in a friendly, customer service oriented manner.

Organisations procure and train behavioural detection because ultimately, they want to disrupt terrorists and wider criminality by detecting them. However, the site or organisation considering behavioural detection should think beyond just detection, as there are two other key elements of disruption that can be readily achieved by a site or organisation: DENY and DETER. This is encapsulated in CPNI's 3Ds disruption model in Figure 1.

Figure 1:
The 3Ds disruption model



2 The role of behavioural detection in protective security

DENY:

Organisations should aim to deny a hostile's ability to gain useful, credible information that can help them plan effective attacks or other criminal activity. This includes information that can be found online, for example an architect's exact floor schematic of a venue, which reduces the need to go to the site to determine this information. This can be readily achieved by auditing and adapting an organisation/site's communications and digital footprint to ensure that this kind of information cannot be accessed. Sites should also aim to deny the hostile's ability to operate effectively at the site itself – where they can collect information needed to plan an attack. This can be achieved by proactive, friendly engagement by staff, which can maximise the hostile's fear of detection via the organisation's capabilities (such as staff, CCTV, police and other security measures). When the hostile is aware of and/or has sight of these, this can increase their levels of anxiety and cognitive workload as they need to look out for and counter these security measures, which can also help DETER them from continuing these activities. Communications can be used strategically to help with this, by highlighting capabilities in place that can lead to the detection of hostile activity.

DETECT:

Organisations should aim to set up security measures and develop capabilities that focus on facilitating and optimising the detection of suspicious people and activities. This is achieved by providing integrated, effective detection capabilities focussed in the right areas at the site (e.g. where hostiles will have to come to obtain information during reconnaissance, or where pickpocket observation points are). These capabilities include: trained specialist staff, well-positioned CCTV and control room (with operators proactively looking for suspicious activity in areas hostiles are more likely to be), staff who have a customer engagement role, and other staff and the public/venue visitors who are enabled to be vigilant, detect and report concerns via an effective reporting and review system.

DETER:

Deterrence is primarily achieved through corporate communications that regularly promote effective DENY and DETECT capabilities at a location, without including any detail that could enable hostiles to counter them. Simple messaging can deter hostiles, and inform, reassure and help recruit the public and staff to assist with detection efforts.

2 The role of behavioural detection in protective security

A venue may have an effective behavioural detection capability and/or staff who are vigilant and take appropriate action – by seeking to identify suspicious activity as well as dealing with any public reports relating to such activities. However, if this is not visible and/or promoted publicly, then a deterrent effect is unlikely – as the hostile must be in the right place at the right time to see this in action. By promoting security measures and capabilities at the location and online, the venue can create a strong message and digital footprint that tells the hostile that it is not just police or security that they need to be concerned about: Anyone, anywhere, could detect them – and this will be investigated and resolved by expert security staff or the police. This helps create fear and concern about detection, increasing workload (DENY) and anxiety (DETER and DETECT) in hostiles considering operating at a site, be they terrorists conducting hostile reconnaissance or petty criminals.

CPNI has specific guidance on the 3Ds disruption model and products available to assist sites, such as security-minded and deterrence communication guidance and training. For further information, see https://www.cpni.gov.uk/beyond-perimeter.

CPNI strongly recommends that sites and organisations first consider the 3Ds approach to disruption if they are contemplating developing a specialist behavioural detection capability.

If this is not considered, then sites run the risk of conducting activities that may counter the effectiveness of specialist behavioural detection capability. For example, poor staff behaviours that create a perception of an easy operating environment, and online communications that may give away details of behavioural detection tactics and capability.

Considering disruption as a whole (i.e. the 3Ds model) will help ensure that every aspect of your site and resources are used in a coherent and complementary manner to disrupt hostiles. For example, communications can help deter hostiles at the point of target selection – these can make them feel wary if they decide to operate on site because of the effective capabilities that are there to detect them. Communications should focus on security measures that are actually in place, otherwise a hostile may perceive that information being communicated is false (or fabricated) and will not be deterred.

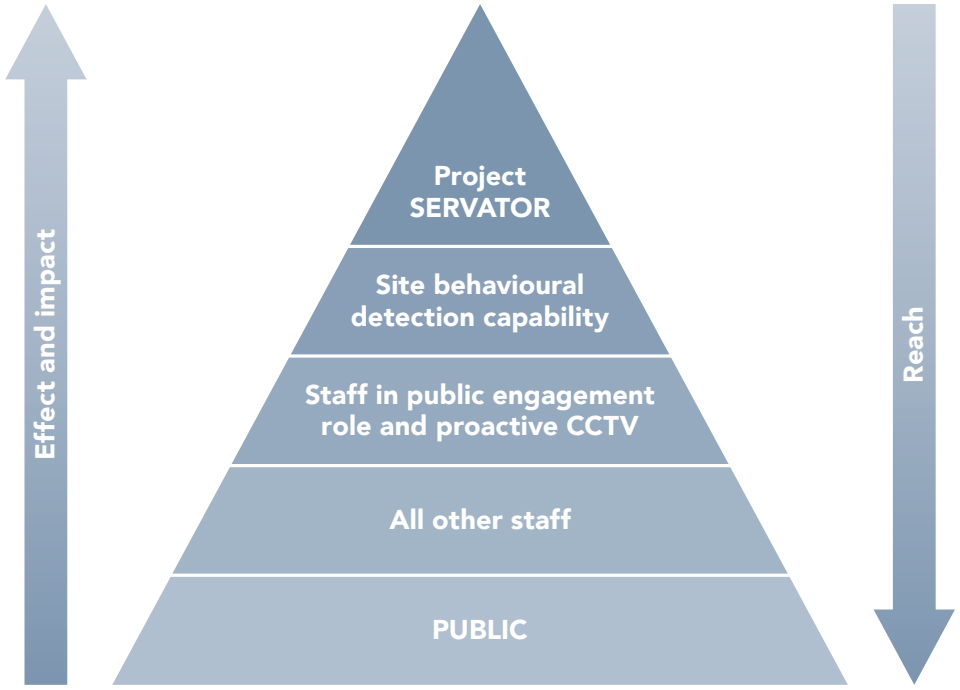
2 The role of behavioural detection in protective security

2.2 The effect and reach of behavioural detection

Staff and the public who are vigilant and report suspicious activity can be a huge 'force multiplier' to complement a limited specialist behavioural detection capability – both in terms of numbers and coverage across the site and times of day – and can help elicit behaviours of concern. For example, in 2015, during a routine security check, a security officer prevented an attacker wearing a suicide belt from entering the Stade de France stadium ground[7]. He was 'just doing his job', but undoubtedly saved lives and mitigated the impact of this co-ordinated terrorist attack.

Figure 2 illustrates CPNI's 'effect and reach' model, which demonstrates using people resource at a site to full effect in order to disrupt hostiles. The further towards the tip of the triangle, the more highly trained and effective the people resource is – but this tends to be very limited in numbers and operation across the site. Lower down the triangle there are greater numbers of people and reach across the site, but these groups are less well trained (e.g. general staff, the public).

Figure 2:
CPNI's 'effect and reach' model



7. https://www.dailymail.co.uk/news/article-3337928/Hero-guard-saved-France-baby-faced-bomber-football-stadium-stopping-sneaking-turnstile-detonating-vest-thousands-fans-President-Hollande.html

2 The role of behavioural detection in protective security

Specialist behavioural detection training typically covers:

- Passive detection – looking for behaviours that may indicate suspicious activities such as conducting hostile reconnaissance or someone behaving atypically from the norm in a particular environment.
- Active detection – using the 'natural' set up of the environment to evoke concern or fear of detection in individuals who have guilty knowledge and hostile intent, such that behaviours (as outlined below) are elicited and are more likely to be displayed in some form (i.e. 'leakage').

Careful consideration should be given to the environment and how the site can be set up. For example, engaging and overt security deployments can be in place at entrance and exit points at a theme park, to observe and potentially influence the responses from people passing through that area. These locations provide 'pinch points' that everyone has to pass through, and therefore provide an opportunity to see if certain individuals respond differently when faced with overt security measures (e.g. canine detection). If it is not possible to set up the environment to help elicit cues, then behavioural detection will be more limited to the passive type outlined above.

Active detection complements measures that aim to DENY and DETER, as this often requires a visible and engaging security presence. Passive behavioural detection is normally more covert and less visible, hence ability to DENY and DETER is more limited. Both approaches require understanding of what is normal for that environment both on that day/time of day, but also in response to the environment set-up.

Section 3:
How behavioural detection works – specialist training

3 How behavioural detection works – specialist training

Table 1 and the following sections of this document provide advice and guidance on what this training should entail and how to obtain it, with a significant focus on specialist behavioural detection training.

Table 1: Capability options that include a behavioural detection component

Capability	Description	Summary of behavioural detection component
PROJECT SERVATOR TOGETHER, WE'VE GOT IT COVERED	National, specialist police capability developed in partnership with CPNI to disrupt hostile reconnaissance and wider criminality via the 3Ds model. Includes specialist behavioural detection capability. For further information see https://www.counterterrorism.police.uk/servator/. Project Servator operates at a range of sites and crowded places across the UK, including events, shopping centres, airports, rail and iconic sites. As such, police may already be deploying Project Servator at a site that is considering the use of behavioural detection and other measures. The deployment of Project SERVATOR and the range of assets used across the UK is effectively managed under a planning and prioritisation process.	Unable to supply for operational security reasons.
Site specialist behavioural detection capability	Specialist behavioural detection officers trained to a high level (as defined in this guidance) to identify and resolve suspicious individuals at a site.	Staff are taught a list of cues, which include behaviours and indicators of concern (e.g. hostile reconnaissance activities and behaviours), and those assumed to indicate emotions such as anxiety and stress due to fear of detection. Cues include: • 'verbal' (e.g. what people do or do not say); and • 'non-verbal' (e.g. facial expressions, body movements, physiological indicators). Good behavioural detection programmes also train people to successfully resolve suspicions, for example, via a 'resolution conversation' or a more formal interview.

3 How behavioural detection works – specialist training

Table 1 and the following sections of this document provide advice and guidance on what this training should entail and how to obtain it, with a significant focus on specialist behavioural detection training.

Table 1: Capability options that include a behavioural detection component

Capability	Description	Summary of behavioural detection component
Staff with a public engagement role/ SCaN for Customer Facing	Staff who can engage with the public, such as roving security personnel and those who act as customer ambassadors. These can be trained to understand what suspicious behaviour may look like on their site, and how to have a polite, but probing, conversation to help resolve suspicions or escalate to a behavioural detection specialist / Project Servator officers (where operational) to resolve.	Staff are educated on the kinds of behaviours and activities associated with Hostile Reconnaissance. For example, people taking particular notice (maybe taking notes or photographs) of security equipment. Staff are also educated on the importance of understanding their own environment and what might be unusual or suspicious activity within this. Staff need to be aware of what is 'normal' and how this can vary according to, for example, the time of day/ week/ year, different locations within their site etc. – in order to detect when something is unusual or suspicious. People are taught to be situationally aware and to report when they detect something 'unusual'. Here the focus is more broadly on 'activities' and 'cues', rather than on specific behaviours. For example, a person loitering in a particular area for a prolonged time for no explicable reason when everyone around them is on the move. SCaN is a free training product available to industry which is delivered against NaCTSO priorities by Counter Terrorism Security Advisors. For further information on this type of training and awareness see: https://www.cpni.gov.uk/security-awareness-campaigns; https://www.gov.uk/government/organisations/national-counter-terrorism-security-office; https://www.cpni.gov.uk/system/files/documents/53/50/Running%20a%20staff%20vigilance%20campaign.pdf For further information on the six SCaN training modules available see: https://www.cpni.gov.uk/Scan
Proactive CCTV control room staff/ SCaN for CCTV Operators/ SCaN for Security Managers	CCTV operators trained to understand when, where and how to proactively look for suspicious activity on their site – that they can refer to roving security personnel and/or behavioural detection specialist / Project Servator officers (where operational) to resolve.	
All other staff/ SCaN for All Staff	Staff with a general awareness as to what suspicious activity and behaviour is at their site, the power of 'hello, can I help you?' in disrupting criminality, and the importance of being vigilant and reporting. The content of this module can also be found in the ACT e-learning https://ct.highfieldelearning.com	
Public and visitors	Public facing vigilance campaigns such as Action Counters Terrorism (ACT) and See it, Say it, Sorted' and other communications to help educate and encourage the public to be vigilant and report suspicious behaviour or activity – as part of their role in helping to keep themselves and the site safe.	

3 How behavioural detection works – specialist training

3.1 Training to spot behavioural cues: Assumptions and limitations

Many providers of behavioural detection training/ capability propose that:

- People with hostile intent will **experience emotions** such as fear, anxiety and stress, because they have 'guilty knowledge' that they are conducting actions which are, for example, illicit and/or illegal, and because they do not want to be caught.
- Hostiles will **exhibit behavioural cues** because of these emotions, for example via facial expressions, body movements, and/or verbal cues.
- These **cues can be reliably observed**.
- Staff **can be taught to detect hostile individuals by looking for these cues**.

This approach is based mainly on evidence from research on detecting deception – how people behave when they are lying and how their behaviour differs to that of people who are telling the truth.

Here there is an assumption that certain cues are a reliable reflection of a person's emotions. However, research has shown that this is not necessarily the case, for example:

Facial expressions may not necessarily reflect how a person is feeling. For example, research has shown that people use their own facial expressions to entice others to engage with them. Therefore, we may smile to invite another person to interact with us, not because we are happy. As such, observing a person's facial expression is unlikely to tell us if that person is experiencing emotions because they have hostile intentions.

Emotional and/or behavioural responses to particular situations will vary between individuals. This can be a result of, for example:

- **Personality differences** (e.g. extroverts seek exciting experiences and need more stimulation to feel excited, so some people may enjoy the thrill of doing something criminal, and be less likely to feel and/or look nervous, fearful)[10];
- **Previous experiences** (e.g. those who have committed crimes before may be more confident and therefore unlikely to feel and/or look nervous)[11]; and
- **Personal preferences** (e.g. people may look nervous in an airport because they are scared of flying, not because they are conducting hostile activities).

10. Ellis, L., Farrington, D., & Hoskin, A. (2019). Handbook of Crime Correlates. New York, NY: Academic Press.

11. Jacobs, B. A., & Cherbonneau, M. (2017). Nerve management and crime accomplishment. Journal of Research in Crime and Delinquency, 54(5), 617–638.

3 How behavioural detection works – specialist training

A number of assessments of this kind of approach have demonstrated that many of the cues people are trained to look for lack any empirical evidence in terms of them being an indicator of hostile intent. Moreover, this approach has the potential for both:

- **'false alarms'** – innocent individuals are identified as potential threats because they are exhibiting behaviours that staff have been trained to look for; and
- **'false negatives'** – individuals with hostile intent are missed because they do not exhibit the behavioural cues that staff have been trained to look for.

Therefore, whilst there is a huge body of research on behavioural cues associated with emotion and deception, when people are being observed in real world environments (e.g. in open, potentially crowded, places) this approach has a high risk of failure, for the following reasons:

3.1.1 Not all hostiles will be or will appear stressed

First, it is incorrect to assume that all hostiles will experience emotions such as fear and stress, and that they will exhibit behavioural cues to indicate that they are feeling this way. **Some criminals and terrorists may not feel nervous if they are confident that they will not be caught, or they may enjoy high stake situations and will therefore not look and/or feel stressed or fearful. This is why the set up and the perception of the environment are vital to consider in any behavioural detection capability.** If the site works comprehensively along the CPNI 3Ds model then it can help create a perception in the mind of the hostile that even a relatively benign environment (e.g. a shopping centre) is actually a high threat environment as there are measures in place to detect them.

In addition, **although hostiles may feel stressed, they can learn ways to manage and conceal their feelings in order to appear confident**. For example, some terrorists and criminals have been known to take drugs in an attempt to calm themselves and conceal signs of nervousness or fear[12].

12. Jacobs, B.A. & Cherbonneau, M. (2017). Nerve management and crime accomplishment. Journal of Research in Crime and Delinquency, 54, 5, 617-638.

3 How behavioural detection works – specialist training

3.1.2
Not all stressed people or people exhibiting particular behaviours are hostile

Some innocent individuals may be mistaken for being a hostile, because they are experiencing certain emotions and exhibiting behaviours that staff have been trained to spot. This issue is particularly relevant in crowded environments, which may be inherently stressful for some people. For example, at a music event, people may be worried when they see security processes in place and/or they may dislike crowded spaces. Moreover, if staff engage with innocent members of the public in a negative way that results in a poor customer experience, this can damage an organisation's reputation. **This is why it is essential to (a) understand the baseline of what is normal for an environment, and (b) follow up any concerns and suspicions with a 'resolution conversation'.**

A resolution conversation is a polite and friendly discussion that involves staff asking probing questions to understand why an individual is behaving in a certain way. Questioning can involve something as simple as asking if the person of concern is okay, or if they need help. The member of staff needs to actively listen to and observe how the individual then responds. If concerns are not resolved and there is no innocent, credible explanation for the behaviours that led to the detection, the member of staff should follow their organisation's process for responding to threats and raise an alarm.

3 How behavioural detection works – specialist training

3.1.3
Even if behaviours are evoked and observable, they may not be seen.

Even if people do feel certain emotions, and exhibit behavioural cues and associated indicators, these cues may not be observable/ seen by others, even when they are trained to do so. That is, behavioural detection is not an 'all seeing, all knowing' capability. It is limited by the attention of the trained observer and what is going on in the environment at the time. It should be noted that:

- **Some cues are hard/ impossible to spot especially from a distance and when it is busy or quiet.** For example, when there is a large crowd at an iconic site where a lot of people are taking photographs, this will make it difficult to spot a hostile taking pictures as part of their hostile reconnaissance activities.
- People may find it difficult to remember all of the cues that they have been taught to look for, therefore they may be more likely to resort to looking for cues they find easiest to remember and/or spot. **This can lead to critical biases such as a reliance on stereotypes of what they believe a hostile is likely to look like.**
- Some behavioural detection training includes 'micro expressions' on the list of cues to look for. However, these are by definition 'micro' (i.e. very subtle) – and therefore most cannot be detected at a distance, and are often said to be hard to detect even during a close-up conversation. Some micro expressions last only a fraction of a second, and as such, can only be observed when watching recorded video that has been slowed down. **Therefore, detecting hostile intent via micro expressions is not practical in real-world situations, especially in large, crowded places. There is also a lack of evidence that technologies can detect hostile individuals via micro expressions, even when they are designed to do so and advertise that they can.**
- The hostile actor may simply be out of sight (e.g. hiding from, or in an area where there is no behavioural detection capability).

3 How behavioural detection works – specialist training

3.2 Addressing the limitations of this approach

When seeking to detect hostile actors via their behaviours and activities we need to consider the following:

- **We need to understand how a particular individual of interest usually behaves in the context that you are observing them in:** This can vary dramatically depending on a range of contextual factors. If you do not have this 'baseline', you cannot detect when someone is acting out of the ordinary.

- **Rather than providing a list of behaviours to look for, training and guidance should provide 'hand holds'** – these are examples of the kinds of things that might be unusual in a specific environment and context – as this is more likely to be an effective behavioural detection approach. 'Hand holds' may include looking for people: with an unusual appearance/attire or belongings (e.g. different to the majority of people in the same context), expressing extremist views, or making threats; loitering near staff-only areas or outside normal dwell zones; seen in multiple areas, outside of a usual journey or work pattern or timeline; attempting to photograph or film security areas or taking measurements/notes of their surroundings; and/or acting in a furtive or secretive manner (avoiding security personnel, CCTV, eye contact or interaction with others), engaging with staff to ask probing or inappropriate questions (e.g. about security measures and staff routines).

- **It is vital that any behavioural detection training includes techniques for successfully resolving suspicions, rapidly and effectively in a short and friendly interaction** – because the majority of behavioural detections are likely to have an innocent explanation. **Without this, suspicions will not be resolved and an innocent member of the public may be made to feel they have been treated like a criminal.**

Section 4:
How behavioural detection works for wider staff and public

4 How behavioural detection works for wider staff and public

4.1 What to look for

An alternative (or complementary) method to detect hostiles is to enable people (staff and the public) **to learn, be aware of and look out for:** (a) What is 'usual' for their environment, and how this varies according to context; and (b) When something looks or feels 'unusual' for that context.

4.2 Looking for the unusual: Strengths of this approach

This approach does not assume that hostile individuals experience and exhibit signs of certain emotions, and has been developed and applied to different environments (e.g. on trains and at bus stops and stations) as a key part of a range of security measures (e.g. the 'See it, Say it, Sorted' DfT campaign).

Rather than training people to look for specific behavioural cues (as described in Section 3.1), facilitating the reporting of anything unusual may be a more effective approach to detect hostile acts, as it is more encompassing and does not focus on specific behaviours. Something 'unusual' might include unusual clothing (e.g. a padded jacket on a summer's day), or a vehicle parked in an unusual location. These examples demonstrate how the concept of looking for the unusual is likely to be more effective in detecting hostiles compared to relying on a list of behaviours:

Wearing a padded jacket could not be included on a generic list of 'behaviours' to look for, but when observed in context may help in detecting a hostile[14]. Otherwise there is a risk that people will rely on 'mental shortcuts' (e.g. stereotyping) to detect potential hostiles.

This approach overcomes the issue of behaviours being context-specific. Whereas looking for behavioural indicators of emotions can be affected by the context (e.g. how confident and experienced the hostile is, how nervous and stressed the non-hostile individuals in the same environment are likely to be), this approach relies on people (staff and the public) having intrinsic and 'expert' knowledge of their environment and knowing when things look or feel out-of-place within that context. For example, what passengers usually do at a train station may vary depending upon the station, time of day and day of week.

14. https://www.independent.co.uk/news/world/europe/istanbul-airport-attack-ataturk-suicide-bombers-images-video-latest-news-a7110536.html

4 How behavioural detection works for wider staff and public

4.3 Responding to suspicions

The public should be encouraged and enabled to report (e.g. directly to staff, via a telephone call or mobile text message to appropriate authorities) and where possible, thanked for making the report. People can be encouraged and enabled by **promoting reporting as a 'civic duty'** – that can benefit themselves and others, **enabling people to be capable of reporting** and ensuring **that they are confident to report and are assured that their concerns will be dealt with appropriately.** This relies also on the organisation taking appropriate and timely action to investigate and resolve these reports, and to give feedback where possible to demonstrate that reporting is acted upon proportionately and appropriately. For further information and products see:

https://act.campaign.gov.uk/

When someone or something unusual is identified, staff should attempt to resolve their concerns via a follow-up interaction or escalate as required, as quickly as possible. Organisations also need to have in place an effective system to investigate reports such that they do not go into a 'black hole'. For example, if a member of the public reports to a member of staff, that employee needs to understand the importance of investigating or escalating immediately, and that there is a system in place that will seek to investigate and resolve the report. Ideally organisations should 'stress test' this system by 'mystery shopping' – deliberately planting a suspicious activity report from a 'stooge' member of the public via various mechanisms to ensure it is enacted on. Revisions to the system can then be made if required.

It is vital that sites have controls in place to stop someone carrying out an inappropriate action, for example calling 999, unlawfully detaining someone or in a worst-case scenario assaulting a member of the public.

Section 5:
Key components of good, specialist behavioural detection

5 Key components of good, specialist behavioural detection

5.1 Key considerations

What are your goals and priorities?
In terms of whether you are trying to detect, deny and/or deter the hostile and the current threat for your environment. For example, your priority might be to deter low level crime in a shopping centre, in which case specialist behavioural detection may be considered unnecessary. Or you might be responsible for detecting more serious criminal or terrorist activities at a tourist site, in which case specialist behavioural detection may have some benefit.

What is your environment?
Does it lend itself to behavioural detection via measures already in place (e.g. airport style screening) or will you need to put more dynamic measures in place to shape the environment to help elicit behaviours of concern? For example, via communications and deployment of visible security/customer engagement assets?

What are your available resources?
The potential success of behavioural detection may rely on factors such as how many staff you have, available budgets for staff and levels of training, the size of your location and the potential reach and impact of those who are trained.

Is your capability able to coordinate and integrate effectively with other measures?
To have maximum benefit, behavioural detection capability must coordinate with other security capabilities in place (e.g. Project Servator deployments (where operational), links to CCTV Control Room Operatives etc.). If you have staff and public vigilance initiatives in place, are your behavioural detection officers able to rapidly resolve suspicions that are flagged? Do you have the mechanisms in place to support this? For example, when a member of staff raises concern to your control room, the control room will contact behavioural detection officer(s) to investigate and resolve in a timely manner.

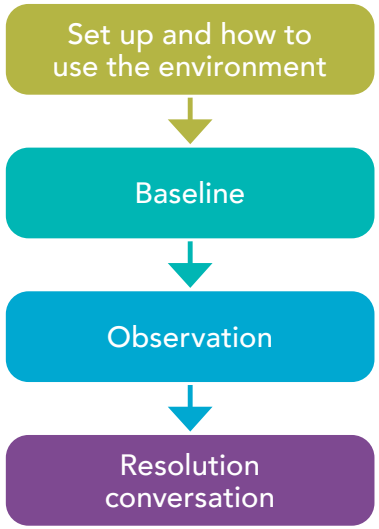
Have you made the most out of your other capabilities to DENY, DETECT and DETER (as outlined in Section 2.1), and are these working in synchrony with your capability and not against it?

Do you have the ability to collate and analyse evaluation measures?
As outlined previously, this is vital to know if your behavioural detection capability is working effectively and to defend it against any accusations of profiling particular groups or individuals (see Section 7 for guidance on evaluation).

5 Key components of good, specialist behavioural detection

5.2 Training components

Below illustrates the key components of good and comprehensive behavioural detection training.



Set up and use of the environment – If behavioural detection is likely to be 'Active', then training should include how to set up the environment, in order to stimulate fear of detection and to facilitate observations that might lead to detection. If more 'Passive' it should still include consideration of how and where the 'natural' environment may elicit behaviours and where, when and how a hostile is likely to operate. For example, when conducting hostile reconnaissance at a site, a hostile is most likely to be in areas where they can collect key information – e.g. staff movements around an entrance. As such, behavioural detection capability can be deployed strategically to maximise opportunities for staff to observe hostiles, and for hostiles to see staff in action.

Baseline – Training must include the importance of understanding the norms of the environment, and how to determine what might be unusual or suspicious in that environment – with and without any 'active' set up. Without this vital component, there is a high likelihood of false positives and negatives.

Observation – Training on how to recognise cues, why they may be exhibited (above and below the baseline) and how to determine the threshold of when this can be categorised as suspicious and worthy of further investigation. This should also include potential errors in observation and how to be aware of and mitigate these.

Verbal cues – What people say and how they say it can be one way to detect hostile individuals, for example if they struggle to answer questions that should be easy to answer, if their 'story' doesn't make sense or if they contradict themselves. In contrast, relying on non-verbal cues (e.g. if a person seems anxious or scared) is likely to lead to false positives and false negatives.

5 Key components of good, specialist behavioural detection

Resolution conversation – Training should include how to have friendly, polite but probing conversations via a short interaction in order to resolve suspicions. This is absolutely essential to the success of any behavioural detection capability. Without it, the potential for damaging false positives (e.g. members of the public who may be showing signs for innocent reasons) and missing true positives (letting someone with malicious intent go) is high. These kinds of conversations provide customer service to innocent members of the public, can increase customer satisfaction, and may lead to staff helping people who may be distressed because, for example, they are lost, late, or have mental health issues.

5.3 Developing and maintaining capability

Behavioural detection is a specialist skill – not everyone can do this – and it is one that needs to be practiced regularly so that skills are maintained. **It is important to note that staff who have undertaken only basic security awareness training should not be referred to as trained behavioural detection personnel.**

People with the necessary attributes (e.g. having natural observation and personal interaction skills) will perform more easily and effectively, and therefore training selection should seek to identify those with these skills and filter out those who do not enjoy interacting with the public.

Once trained, specialist skills then need to be maintained. As with any specialist skill, trained people need use their skills on a regular basis to ensure currency, and continued professional development is essential.

Evaluation is also essential – recording and analysing the outcomes of behavioural detection, both positive and negative, is vital to determine if training has been of benefit and if the capability is deploying to good effect (and therefore worthy of continued development and investment). Evaluation is also needed to ensure that it is not accidentally biasing or profiling certain visitors at a site (e.g. based on their gender, race or mental health issues). Indeed, reliable data is vital to defend the capability, should staff decisions and responses based on behavioural detection ever be raised, challenged or questioned.
See Section 7 for further insight into evaluation.

Section 6:
Procuring specialist behavioural detection training, technologies and tools

6 Procuring specialist behavioural detection training, technologies and tools

There is a range of behavioural detection capabilities available, in terms of training, technologies and tools. These vary dramatically in terms of their objectives, approaches and methods, and in terms of their effectiveness and successful implementation.

Companies should provide training that follows the structure and content outlined in Section 5.

Behavioural detection that does not include a resolution conversation to resolve suspicion should be avoided due to risk of false negatives and positives. Staff should be trained to interact with the public. Moreover, at sites where persons of concern can be/need to be interviewed, specialist staff should be trained in (i) how to effectively interview, (ii) how to look for cues of deception, and (iii) how to elicit cues of deception.

When considering behavioural detection training, companies should be required to provide evidence of how their approach and methods are applicable to: (i) requirements and environment; (ii) available resources; and (iii) existing measures and processes. They should also set out a clear plan of how they will measure (and/or how they will help to measure) and demonstrate success and impact.

Companies should be able to provide quantifiable evidence of the effectiveness of their training – not anecdotal examples or testimonies from satisfied customers – but clear and robust evidence (e.g. data) that demonstrates increased detection performance (after training, compared to pre-training). (Other measures can also be used as evidence of disruption, as discussed in Section 7.)

When procuring equipment and technology, organisations should again require suppliers to demonstrate how this will work for them. Companies should be expected to provide evidence that their product will be effective, and guidance on how this will specifically meet the organisation's requirements. Section 7 provides further details on evaluation of training, technology and equipment.

Procurement decisions should never rely on the background and experience of the supplier (e.g. ex-military / intelligence staff). Moreover, customers should be wary of 'scientific' looking papers and where possible, get these reviewed by a scientist in your team or by an independent expert. **Suppliers should also be required to demonstrate that their products (training/ technology/ equipment) will not have a negative impact on normal site users.**

The Register of Security Engineers and Specialists (RSES) has been established to promote excellence in security engineering and provides a benchmark of professional quality against which its members have been independently assessed. Organisations who supply behavioural detection training are encouraged to engage with this process. It offers potential clients the assurance that registrants have achieved a recognised competence standard through a professional review process.

For details about applying for the register and the application process please see https://www.cpni.gov.uk/register-security-engineers-and-specialists-rses

Section 7:
Evaluating your behavioural detection capability

7 Evaluating your behavioural detection capability

7.1 Key considerations for measuring effectiveness

It is important to understand that:

- **Simply providing staff trained in behavioural detection does not equal success.** Those considering the use of behavioural detection need to identify what they want to achieve (i.e. their 'measures of effectiveness').
- Single measures alone cannot provide a full picture of this: **A range of measures are best; which can then be triangulated to evaluate the impact** (e.g. on-the-spot arrests, number of reports, quality of reporting, number of complaints and other customer feedback).
- **Covert testing can provide insights and evidence of the effectiveness of behavioural detection, but this can be complex and costly** in terms of the time, effort and resources required to organise, run and manage.
- Behavioural detection can be applied to deter and disrupt criminal acts as well as terrorist attacks, but **measuring deterrence is hard, if not impossible, in most real-world contexts**.
- **One preferred proxy measure of deterrence is 'red teaming'.** This is usually delivered by an external company with the relevant skills and expertise to adopt a hostile 'mind-set' and evaluate the security posture and potential vulnerabilities of specific locations and sites.

7 Evaluating your behavioural detection capability

7.2 Evaluating behavioural detection capabilities: A 10-point checklist

Organisations should use the following checklist to ensure that they have sufficient evidence that behavioural detection is suitable and likely to be effective at their site. This can be applied to the procurement of behavioural detection training, technology and/or equipment.

1. Organisations first need to consider what they are seeking to achieve, in order to determine appropriate measures of 'success'/'impact' regarding behavioural detection capability. Organisations also need to consider their available resources, in terms of staff numbers and funding to spend on (i) the initial outlay, (ii) the ongoing maintenance, and (iii) the evaluation of their behavioural detection capability.
2. Organisations should explore different options regarding different behavioural detection products and different potential suppliers. They should discuss their requirements and available resources with potential suppliers. Suppliers should help them identify options and provide advice to help with this decision.
3. Organisations should only consider procuring products (training/ equipment/ technology) that have already been deployed and tested (or at least trialled) at a site similar to theirs (in terms of size, footfall, layout, numbers of staff etc.).
4. Suppliers should be required to describe and explain how they have previously tested/ trialled their product, and the metrics that were chosen to test their product. This could include measuring the number of 'stops' and referrals to the police made by staff trained in behavioural detection, customer satisfaction scores, and a baseline assessment of security measures made by Red Teaming experts.
5. Suppliers should present evidence that they have collected data on their chosen metrics before and after the implementation of their product at a similar site.
6. Suppliers should clearly outline how they collect data on these metrics. For example, self reports from staff and/or the public, observations of staff, data from the police, Red Teaming.
7. Suppliers should demonstrate that they have measured the effectiveness of their product by analysing data collected before and after the implementation of their product. This analysis should show that this resulted in a positive effect (e.g. more 'stops' and referrals, increased customer satisfaction scores, increased deterrence effects as assessed via Red Teaming experts).
8. Suppliers should provide detailed guidance and advice on the best deployment approach for your site, for example, in terms of where and when to deploy their product at the site to maximise its impact.
9. Suppliers should design a plan of how they will trial/test their product at your organisation's site(s).
10. Suppliers should demonstrate how their product is practical, feasible, affordable and proportionate to your organisation's requirements and available resources.

7 Evaluating your behavioural detection capability

7.3 Evaluating the evidence: A final note

It is worth noting that behavioural detection has only been properly tested against criminal activity[16]: As yet, we do not have robust evidence that it can be effective in the detection of terrorists. This is because it is hard to collect data due to the low number of terrorist activities that might actually be observed by those trained in behavioural detection: This has resulted in a lack of quantifiable data on terrorist activities. However, significant effort has been made to understand how lessons from the extensive literature on criminality can be applied to understand and disrupt terrorists. Research has demonstrated that these different types of hostiles think, feel and operate in the same way[17]. We do not yet have significant evidence that behavioural detection can be effective in disrupting terrorist activities. However, our research suggests that it is very likely that it can.

16. https://www.cpni.gov.uk/disrupting-hostile-reconnaissance
17. Unpublished academic research that included an analysis of 90+ terrorist autobiographies and a synthesis of court, police and open-source documents regarding over 100 terrorist plots.

Section 8: Conclusion

Behavioural detection capability has the potential to detect, deter, and deny hostiles from operating in a range of contexts and environments. However, behavioural detection should only be deployed as part of an integrated system to ensure that it complements and is complemented by other security measures. It is important that the set-up of the environment is conducive to and organised in a way that can maximise the potential success of behavioural detection, and that training provides skills and techniques that are evidence-based and tailored for different audiences. Those considering the procurement and deployment of behavioural detection capability should ensure that they do so in an appropriate and proportionate way and have the resources to do so. The guidance provided here aims to assist those responsible for the security of different environments, to ensure that any application of behavioural detection meets requirements, is effective and is successful.