ProtectUK

Hostile reconnaissance

Original publication date
02/11/2020

1. Introduction

Hostile reconnaissance is the term given to the information-gathering phase conducted by those individuals or groups with malicious intent. It is a vital component of the terrorist attack planning process. However, terrorism may not be the only threat a site faces. This guidance therefore uses the term ‘hostile’ to refer any individual or group conducting reconnaissance.

The National Protective Security Authority NPSA (formerly CPNI) defines hostile reconnaissance as ‘Purposeful observation with the intention of collecting information to inform the planning of a hostile act against a specific target.’ Generally, the more sophisticated the attack, the more complex the attack planning has to be. This means more information and reconnaissance is needed.

The information gathered is typically used by hostiles to assess security and likelihood of detection; to assess vulnerabilities in security and the likelihood of success. Information about a site or event may be gained through online research, conducting on-site visits and, where possible, through insider knowledge. The hostile will try to obtain detailed information to sufficiently inform their method of attack and increase the likelihood of success.

Remember:

- you cannot spot a hostile from their appearance, age, ethnicity, gender or clothing, but you can identify and report suspicious behaviour
- stopping a hostile before they can carry out their plans will ultimately save lives

Objectives of hostile reconnaissance



2. How do you identify suspicious behaviour?

You must understand what is normal and what is ‘every day’ behaviour. Take the time to understand your working environment, your regular commute, your daily routine and the people and activities you see most often. Learn to spot the difference between normal and unusual or suspicious behaviour. Be alert to the threat.

Questions you should ask yourself if you believe someone is acting suspicious include:

- Is that person really taking a selfie or a photograph of something else?
- Are they loitering in restricted or non-public areas?
- Are they paying significant interest to entrances, exits, CCTV cameras or security features or staff?
- Are they asking unusual questions?
- Are they concealing their faces or in disguise?

It is not just people on foot; vehicles are often used by hostiles planning attacks. Be aware of vehicles parked out of place, abandoned, or a vehicle retracing the same route.

Challenging and reporting suspicious behaviour

After conducting a dynamic risk assessment: You SHOULD approach a person that has been acting in a suspicious manner and politely ask them to account for their actions.

- Always remember - Stopping a hostile before they can carry out their plans will ultimately save lives

- You cannot spot a hostile from their appearance, age, ethnicity, gender or clothing

- You can identify and report their suspicious behaviour

What information do the police need from you?

If you become aware of suspicious activity, you should dial 999 if the person is still on scene and you need an immediate police response.

The following details will be useful to provide to the police:

- When did this happen? Provide an accurate date and time of the incident
- Where did this happen? Describe the venue, address and specific details about the location
- Who did you see? Give a detailed description of the person and what they were wearing and/or the vehicle they were in, and the direction of travel. The name, date of birth, address, and any phone numbers obtained of the person if they were stopped
- Why you thought it was suspicious?
- What actions you took at the time?

Remember: It is always better that police are called while the person or vehicle is still at the scene. If the person has left the scene and the route they took is unknown, or a significant period of time has elapsed since the incident, then contact the Anti-Terrorist Hotline on 0800 789321 or report online or 101.

Security staff powers

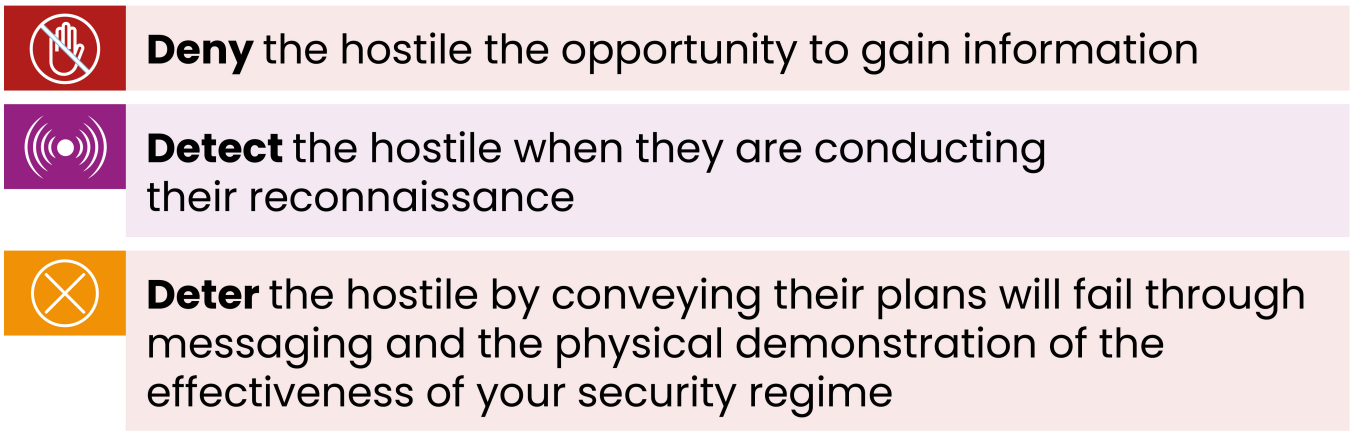
If part of the suspicious behaviour involves the taking of photographs, understand your powers:

- There is NO law that prevents a person from taking a photograph of anything or any person in a public place
- There is NO legal power to require or ask that any images taken are to be deleted
- Security personnel have NO legal power to ask to view images taken

- Security personnel have NO legal power to seize any camera or phone used to take any image
- If police are called, a person CANNOT be detained by security staff awaiting the arrival of police
- Powers to search and seize are ONLY available to a police officer

3. Security managers

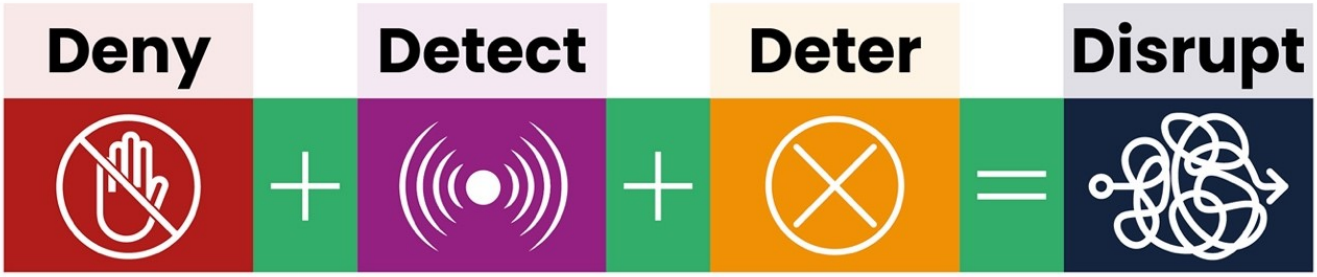
What are you trying to achieve?



This approach will disrupt the hostile's plans and play on their concerns of failure and detection.

The key to disruption comes from understanding the information the hostile needs, where they are going to have to go to get this information, as well as the hostile's mind-set (how far they will go to get the information they need). Once this is understood, an organisation can shape its protective security and other resources, such as corporate communications and employee behaviours, to help disrupt hostile reconnaissance.

Remember: Deny + Detect + Deter = Disrupt



DENY them of the information they want to gather

Denying the hostile of information they need to fulfil their information requirements is the first step an organisation can take in forcing the hostile to either disregard their site as a target, or by making sure that they have to undertake further, potentially detectable, reconnaissance. For example, removing or modifying information from public-facing websites and educating employees on what kind of information hostiles will be looking to use (from their social media accounts, for example).

Denying the hostile of information they need can also mean creating uncertainty and unpredictability about security arrangements at a site. For example, unpredictable timing, type and location of security patrols makes it difficult to assess a pattern of activity that they can exploit with any confidence.

DETECT the hostile and understand their state of mind

Hostiles know they are on site for malicious reasons and that their behaviour might appear out of the norm. This makes them more anxious or paranoid and therefore, potentially susceptible to detection. This natural anxiety can be amplified by communicating and demonstrating an effective range of detection security measures at the site. Vigilant and engaged security officers with timely and appropriate interventions can be particularly powerful, in addition to well-sited CCTV and control rooms with proactive operators looking for suspicious activity.

DETER hostiles with strong demonstrations of physical security measures

Deterrence is a vital component of disrupting hostile reconnaissance for the majority of sites and organisations. It is the main desired effect of their protective security against hostiles.

NPSA (formerly CPNI) defines deterrence as ‘The intelligent, co-ordinated promotion of protective security provision to the hostile that results in the perception and/or assessment that the reconnaissance or the attack itself will fail.’

This is about proactively marketing to hostile audiences your site's protective security measures, primarily an organisation's **DENY** and **DETECT** capabilities. The fact that the hostile is actively seeking information on the security measures at a site can actually be used to deliver that very same deterrence message. If an organisation does not proactively promote its **DENY** and **DETECT** capabilities to hostiles, then it is missing an opportunity to disrupt hostile reconnaissance. The hostile may visit a site several times both physically and online, so it is important that proactive marketing of your sites protective security messages is maintained. Such messaging needs to be carefully balanced, as too much specific security detail could help attack planning.

Crucially, an organisation should have an excellent employee vigilance and reporting culture that is clearly evident in the immediate reporting of suspicious behaviour and the speedy response of security personnel.

Hostile reconnaissance checklist

When an organisation is clear on the nature of the threats it faces, and has understood the **deny, detect, deter** principles, then vulnerability to online and physical hostile reconnaissance can be reduced by considering the following six themes:

- Having a secure online presence
- Operating a robust entry process
- Understanding the hostile reconnaissance threat
- Having a strong staff security awareness
- Operating with vigilant and professional security
- Having a deterrence strategy

4. See Check and Notify - SCaN

See, Check and Notify (SCaN) aims to help businesses and organisations maximise safety and security using their existing resources. Your people are your best asset in preventing and tackling a range of threats, including terrorism, criminal activity and protest. SCaN helps ensure that individuals or groups seeking to cause your organisation disruption and/or harm are unable to get the information they need to plan their actions. It also empowers your staff to know what suspicious behaviour to look for, and what to do when they encounter it. Additionally, the skills they learn will help them to provide a better customer experience.

5. Project Servator

Project Servator is a strategic method of policing designed to deter, detect and disrupt a wide range of criminal activity, ranging from pickpocketing and property theft, to terrorism. Project Servator provides a reassuring presence for the public and the communities it serves. Deployments are unpredictable and intelligence-led, arriving unannounced at any time, and lasting for differing amounts of time. They involve uniformed and plain-clothes officers working together with other specially trained officers.

6. What is insider threat?

Deliberate insider

A hostile who obtains employment with the deliberate intent of abusing their access.

Volunteer/self-initiated insider

A hostile who obtains employment without deliberate intent to abuse their access, but at some point, personally decides to do so.

Exploited/recruited insider

A hostile who obtains employment without deliberate intent to abuse their access, but at some point are exploited or recruited by a third party to do so.

Accidental insider

Staff who by their actions might inadvertently leak information, either because they haven’t received adequate training, or because they have been asked to undertake an action that they don’t recognise as being something they shouldn’t do.

If the hostile is unable to gather the information they require from online or on-site reconnaissance,

they may attempt to recruit an insider to help them achieve their aims.

To help mitigate the threat of insiders, a range of personnel security guidance is available from NPSA (formerly CPNI) or your CTSA, based on the following four components:

- Personnel security risk assessment
- Pre-employment screening
- Ongoing personnel security
- Strong security culture

When applied consistently, personnel security measures not only reduce operational vulnerabilities, they can also help build a hugely beneficial security culture at every level of an organisation.

Robust personnel security helps organisations to:

Employ reliable people to minimise the chances of staff becoming unreliable once they have been employed
Detect suspicious behaviour and resolve security concerns once they emerge

Examples of ‘insider activity’ include:

- Unauthorised disclosure of sensitive information to a non-entitled third party
- Process corruption (illegitimately altering an internal process or system to achieve a specific, non-authorised objective)
- Facilitation of third-party access to an organisation’s assets (including premises, information and people)
- Physical sabotage, including theft
- Electronic or IT sabotage

Further information

Go to the NPSA (formerly CPNI) Understanding Hostile Reconnaissance webpage for further information on this topic.

KEYWORDS

CPNI

HOSTILE RECONNAISSANCE

SUSPICIOUS BEHAVIOUR

SECURITY

RISK

PERSONNEL SECURITY

PALS GUIDANCE

NPSA

PALS

PUBLICLY ACCESSIBLE PLACES

PUBLICLY ACCESSIBLE LOCATIONS