CPNI
Centre for the Protection of National Infrastructure

HOSTILE RECONNAISSANCE

Understanding and countering the threat

June 2016

Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer or otherwise, does not constitute or imply its endorsement, recommendation, or favour by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

Contents

Overview and aim of this guidance

Hostile reconnaissance, the term given to the information gathering phase by those individuals or groups with malicious intent, is a vital component of the attack planning process.

Based on over five years of research and extensive testing and evaluation, this guidance gives security managers an understanding of why and how hostile reconnaissance is conducted, and the principles of how to disrupt threats during the reconnaissance phase, along with practical measures on how to reduce the vulnerability of their site.

Critically, the approaches and suite of tools provided in this guidance have been carefully developed to disrupt hostile reconnaissance while having a neutral, informing or even reassuring and recruiting effect on the normal site user. They also focus on utilising existing protective security resources such as CCTV control rooms, security officers and other important resources, such as corporate communications and employees, more effectively to disrupt hostile reconnaissance.

This guidance first provides an overview of hostile reconnaissance in the context of the attack planning process: how to consider the threats an organisation faces from this perspective, the hostile's information requirements, where they will get this information from and how they feel when doing so.

With this understanding, the guidance then provides the Centre for the Protection of National Infrastructure's (CPNI) principles of disrupting hostile reconnaissance: **Deny**, **Detect** and **Deter**. It explains how understanding these, in combination with a recognition of the threat, can help determine an organisation's current vulnerability to hostile reconnaissance and what can be done to counter this.

The final section includes a checklist to provide a method of assessing a site's vulnerability to hostile reconnaissance.

This guidance uses the term 'hostile' to refer to the individual or group conducting the reconnaissance.

Hostile reconnaissance: understanding the threat

Parties conducting hostile reconnaissance; its place in the attack planning process and the opportunity to disrupt.

Organisations face a variety of threats: terrorists, activists, corporate or state-sponsored spies and criminals scrutinise potential targets from near and far.

But while these threats and their aims may vary, hostiles are united in their desire to succeed. Recognising they may not get a second chance to achieve their aims, hostiles will typically plan carefully.

By using online research, on-site visits and, if and where necessary, insider knowledge, the hostile will try to obtain enough detailed information and get sufficient certainty about the reliability of this information to inform their modus operandi and be sure of success.

This activity can be described as hostile reconnaissance. CPNI defines it 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, and consequently the greater the information requirement and reconnaissance need. The information gathered is typically used by hostiles to assess the state of security and likelihood of detection; to assess vulnerabilities in security and to assess likelihood of success.

Understanding this gives security managers an absolutely crucial opportunity to disrupt by creating a perception and/or assessment of failure by hostiles in two main ways:

- denying them the ability to obtain the information they need from their research because they simply cannot obtain it, or they could but the risk of detection to achieve this is too high
- promoting failure – both of their ability to conduct hostile reconnaissance (they will not be able to get the information, they will be detected) and of the attack itself

These effects can be achieved because in the process of conducting hostile reconnaissance the hostiles are making themselves vulnerable – they are online and at the site looking for and obtaining this vital information.

Protective security can therefore be focussed in the following manner: to *deny* the hostile the opportunity to gain information, to *detect* them when they are conducting their reconnaissance and to *deter* them by promoting failure through messaging and physical demonstration of the effective security. This approach will play on their concerns of failure and detection.

The key to disruption comes from understanding the information hostiles need, and where they are going to have to go to get this and their state of mind. This, in turn, is dependent on understanding the threats in a way that enables prediction of likely attack scenarios.

Understanding the threat

It is important that an organisation understands the threats it faces. Not all threats are applicable to all organisations so it is important that a security department understands what it is defending against.

While an organisation may face a variety of different threats with different attack scenarios, there are likely to be commonalities in information requirements across these. Therefore measures put in place to disrupt hostile reconnaissance can be effective over a wide range of threats.

Given that not all threats are the same, a useful way of understanding those particular to an organisation is to consider the mindset of the hostile.

A hostile's mind-set is determined by Intent, Capability and Culture. By understanding this, together with the assets you are trying to protect, you can understand likely attack scenarios.

Intent	This is what the hostile wants to achieve. Think about their overall aim as this will help identify the effect the hostile wants the particular attack to have
Capability	This is about the resources at the hostile's disposal. Think about equipment, time, personnel, skills and training, financial backing and geographic location
Culture	This is the hostile's personal motivations and appetite for risk

A security manager may not be able to answer every question relating to a hostile's mind-set but by attempting to understand it they can better determine likely attack scenarios, and therefore what information is needed, and where they will go (online, onsite, inside knowledge) to get this.

Security managers should revisit and update these scenarios regularly as their understanding of their threats evolves. As each route is closed to hostiles, the more motivated and those flexible in time and resources may continue to look at alternative ways to achieve their aims, including the use of insiders (those that use their legitimate access to an organisation to cause harm).

Conducting this assessment across all the main threats will enable an organisation to identify commonalities in information requirements. This assessment will enable the security manager to focus their protective security measures, whether cyber, personnel or physical, more effectively to disrupt a range of hostile groups and to be as effective as possible if the threat increases.

The next section will examine the principles of countering hostile reconnaissance.

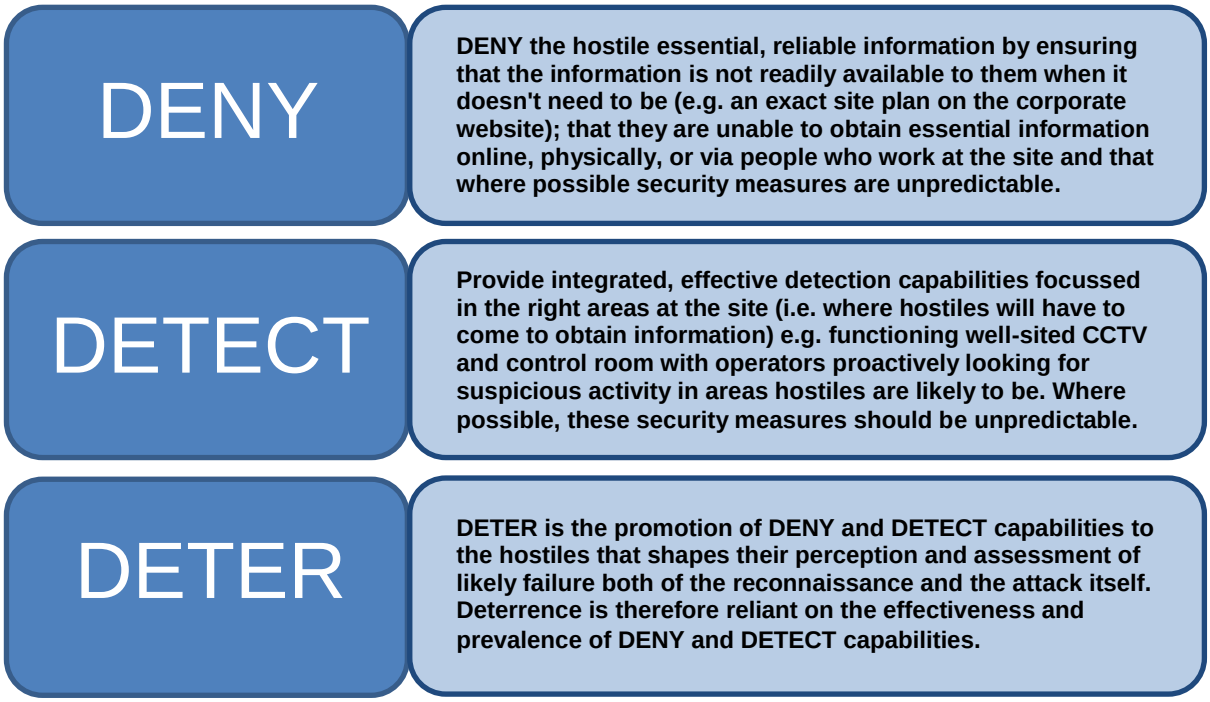
Countering hostile reconnaissance: the principles

Understanding the threat can allow a security manager to determine:

- what information the hostiles will be looking for and why
- where the hostiles will go to obtain this information
- the hostile mindset: how far they will go (effort and resource, motivation and risk appetite) 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. This section describes what these principles are, how they work to disrupt hostile reconnaissance and how they can be applied in terms of activties at a site.

CPNI research has shown that there are three principal ways that this can be achieved – **DENY**, **DETECT** and **DETER**:



The diagram on page eight illustrates the relationship between these three key components of disruption and, if done well, the effects of these on the mindset and assessment of the hostile.

DENY them what they need

Denying the hostile the information they need to fulfil their information requirements is the first step an organisation can take in forcing the hostile to either disregard them as a target or ensuring that they have to undertake further, potentially detectable, reconnaissance.

Removing or modifying information from public-facing websites and educating employees on what kind of information hostiles will be looking to harvest from, for example, their social media accounts, is a simple yet efficient means to deny the hostile what they need.

Denying what 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 determine a pattern of activity that they can exploit with any confidence.

DETECT and the state of mind of the hostile

Detection and the promotion of integrated, effective capabilities, such as vigilant and engaged security officers with timely and appropriate response, can be particularly powerful. This is because hostiles operate with a different mindset to the normal site user. They know they are on site for malicious reasons and they know that they be might behaving in a way that is out of the norm, thereby making them more anxious or paranoid and therefore potentially susceptive to detection.

This natural anxiety can be amplified by communicating and demonstrating the range and effectiveness of the detection capabilities at the site. This is the vital function of deterrence.

DETER - generating and sustaining deterrence

Deterrence is a vital component of disrupting hostile reconnaissance. Deterrence is, for a majority of sites and organisations, the main desired effect of their protective security on hostiles. In many cases it is assumed that because protective security measures are in place they are, by default, deterring. To get the most out of deterrence for a site requires proactive effort by the organisation.

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** protective security provision, primarily an organisation’s DETECT and DENY capabilities, to the hostile audience. Hostiles are looking for critical information and evidence about these measures online and at the site to help inform their attack planning.

As such, the fact they are actively conducting information gathering activities (i.e. that they are ‘tuned in’ to information about security measures and state of security at the site) can be used as a way of delivering deterrent messaging to them.

The messages, such as the one illustrated to the right, should convey that these capabilities are in place and that they will be unable to gain access, or have sufficient confidence in the information essential for attack planning without an unacceptable risk of being detected.

The importance and benefits of deterrence

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 organisation loses the chance to get the hostile to discount a site as a target at the initial target selection phase (which may be conducted primarily online), or at least prime them to be anxious and concerned about being unable to gain access and be detected when conducting physical reconnaissance.

For example, an organisation may have an excellent employee vigilance and reporting culture, with staff reporting in suspicious activity immediately and security officers officers responding rapidly. This can be hugely deterring to the hostile – it's not just CCTV and security officers they need to worry about spotting them, everyone could be watching.

These effects work for a multitude of protective security capabilities. Of course, this has to be done carefully and needs to be achieved in a way that doesn't give hostiles the information they are looking for.

How to proactively promote DENY and DETECT capabilities to DETER

How an organisation provides its messages and evidence of these capabilities needs to be done carefully and thoughtfully. For example, being considerate of the normal site user and their perceptions of such messages (ideally to be reassuring and informative or to have a neutral effect), and critically, to convey the protective security without giving away detail that could be helpful to hostiles

It is important to see this not just as a one-off requirement. Hostiles will potentially be coming back many times online and at the site, so it is important to keep the 'drumbeat' going in terms of promoting capabilities.

Where possible, use video and pictures – social media is an excellent platform for this – to help provide credible evidence that these capabilities exist and work. For these reasons, 'co-ordinated' is also an important term in CPNI's definition of deterrence. For example, if an organisation has just had CCTV cameras upgraded, there is a perfect opportunity to put out a news story in the publically-available site magazine, informing about its effectiveness but without giving away too much technical information that would assist the hostile.

However there is an important caveat to the promotion of DENY and DETECT capabilities. **Any promotion of capabilities must be truthful.** If it isn't, the hostile will soon uncover this deceit, with the resulting effect of potentially not believing anything that an organisation has highlighted and potentially even motivating them to continue.

Hostile reconnaissance checklist

Once they have understood the threats that they face and the principles of DENY, DETECT and DETER, organisations can help reduce their vulnerability to online and physical hostile reconnaissance by considering the following six themes:

- secure online presence
- robust entry process
- hostile reconnaissance threat is understood
- strong staff security awareness
- vigilant and professional security
- deterrence strategy

When thinking about these, security managers should ask themselves the questions on the following pages and if they are unable to answer them, they should consult the CPNI or the National Association of Counter Terrorism Security Officers (NaCTSO) websites, or they should speak to their CPNI adviser or Counter Terrorism Security Advisor (CTSA).

Question	Yes/No	What will be the result?
Does your organisation think about the information it puts into the public domain and consider what positive/negative impact this may have on those engaged in hostile reconnaissance?		Your organisation considers and manages what information is available about it in the public domain and this will help deter those carrying out online hostile reconnaissance.
Do your employees understand why they need to be aware of what information they reveal about themselves or their organisation when online?		Your employees consider the impact their digital footprint has on both them and the organisation they work for, thereby making it more difficult for hostiles to harvest information from them.
Does your organisation understand the threat posed by employees inadvertently giving away information or allowing unauthorised access or malicious software onto your systems?		Your organisation has an understanding of how spear phishing (and similar) attacks are conducted and what can be done to mitigate them.

Question	Yes/No	What will be the result?
Do your employees undergo identity and document verification training?		Employees tasked with document verification, whether during pre-employment screening and/or during visitor entry, are vigilant to the threat of fraudulent documentation.
Are your security personnel sufficiently motivated to identify, deter or detect hostile reconnaissance?		Motivated, attentive and observant security personnel that can form a highly-effective deterrent presence and final line of defence where other interventions may have failed.

Question	Yes/No	What will be the result?
Do you understand what hostile reconnaissance is, where it may be conducted at your site and what you can do to deter or detect it?		Potential hostile reconnaissance points are identified and mitigation measures introduced.
Do you make use of deterrence materials such as security posters aimed at hostiles, in and around your site?		Security managers are given the materials and support to carry out a deterrence messaging campaign, resulting in the deterring or detecting of hostiles.

Question	Yes/No	What will be the result?
Have you measured your organisation's security culture?		Your organisation understands its security culture and identifies where and why it might need to change.
Do your employees know why they need to be vigilant in and around their place of work?		Employees display vigilant behaviours in and around the workplace, thereby making them less of a target and more likely to identify those conducting hostile reconnaissance.
Have your employees been educated as to why their security behaviours in the workplace matter?		Employees display good security behaviours in and around the workplace.
Do your employees know what social engineering looks like and what to do if they think it is happening to them?		Employees recognise social engineering approaches and respond appropriately.
Do your employees understand why they need to be aware of what information they reveal about themselves or their organisations online?		Your employees consider the impact their digital footprint has on both them and the organisation they work for, thereby making it more difficult for hostiles to harvest information from them.
Do your organisation's line managers understand the role they have to play in security?		Managers consider security while making day-to-day business decisions and ensure their teams are kept up-to-date on security matters.

Question	Yes/No	What will be the result?
Does your security department understand the threats it faces?		Security personnel understand the threats posed to their organisation and are motivated to identify and disrupt hostile reconnaissance.
Do your security personnel display a professional-looking presence, profile and posture?		Security officers are motivated to identify and disrupt hostile reconnaissance.
Have your security personnel received training in detecting suspicious behaviour and tactical questioning?		Security officers can more readily identify hostile reconnaissance and resolve suspicions through questioning.

Do your CCTV operators know what to look for in terms of hostile reconnaissance?		Improved effectiveness of CCTV operators in deterring and detecting hostile reconnaissance.

Question	Yes/No	What will be the result?
Do you make use of deterrence materials in and around your site?		Hostiles are deterred by, or detected as a result of, your deterrence materials.
Are you considering how all the elements of your security and communications assets can be used together when deterring and detecting hostile reconnaissance? Are you intelligently promoting your security measures?		Security managers understand the threat from hostile reconnaissance. Your organisation's security assets are coordinated and utilised to create the maximum effect.

CPNI advice

The CPNI website – www.cpni.gov.uk provides more information on how to deter hostile reconnaissance.

Relevant guidance includes:

Employee Vigilance campaign
Workplace Behaviours campaign
Social Engineering: Understanding the threat
Guard Force Motivation

For more information, please contact your CPNI adviser or CTSA.

Other CPNI products

If the hostile is unable to gather the information they require from their online or on-site reconnaissance, they may attempt to recruit an insider to help achieve their aims.

To help mitigate the threat of insiders, CPNI has produced a range of personnel security guidance products and training based around the following four components:

- personnel security risk assessment
- pre-employment screening
- ongoing personnel security (aftercare)
- 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

- minimise the chances of staff becoming unreliable once they have been employed
- detect suspicious behaviour and resolve security concerns once they emerge

Physical security

CPNI has also produced a range of physical security guidance products and training looking at the following areas:

- chemical, biological, radiological
- CCTV
- explosives and ballistics protection
- hostile vehicle mitigation
- lighting and obscuration
- perimeters and access control
- secure destruction of sensitive items
- search and screening
- physical security over IT

Utilisation of and, where appropriate, demonstration of efficient physical security measures will help with countering hostile reconnaissance.

A good starting point to help plan the implementation of security measures is to read CPNI's Guide to Producing Operational Requirements for Security Measures. This lays out a systematic assessment process and has been successfully used in many organisations.